Nivaldo Cunha Bettencourt da Silva

Segurança no Comércio Eletrónico

O caso de Cabo Verde

Universidade Jean Piaget de Cabo Verde

Campus Universitário da Cidade da Praia
Caixa Postal 775, Palmarejo Grande
Cidade da Praia, Santiago
Cabo Verde

13.9.14

“Os covardes morrem várias vezes antes da sua morte, mas o homem corajoso experimenta a morte apenas uma vez.”

William Shakespeare

Nivaldo Cunha Bettencourt da Silva

Segurança no Comércio Eletrónico

O caso de Cabo Verde

Universidade Jean Piaget de Cabo Verde

Campus Universitário da Cidade da Praia
Caixa Postal 775, Palmarejo Grande
Cidade da Praia, Santiago
Cabo Verde

13.9.14

Nivaldo Cunha Bettencourt da Silva, autor da monografia intitulada Segurança do Comércio Eletrónico – O caso de Cabo Verde, declara que, salvo fontes devidamente citadas e referidas, o presente documento é fruto do meu trabalho pessoal, individual e original.

Cidade da Praia ao 30 de Janeiro de 2014
Nivaldo Cunha Bettencourt da Silva

Memória Monográfica apresentada à Universidade Jean Piaget de Cabo Verde como parte dos requisitos para a obtenção do grau de Licenciatura em Engenharia de Sistemas de Informática.

Sumário

Com a necessidade de expandir o negócio juntamente com a expansão da *internet* e do surgimento de novas tecnologias, surgiu o comércio eletrónico cujo objetivo é facilitar os processos de compra e venda sem a necessidade de construção de novas instalações visto que o mesmo pode ser expandido, a nível mundial, através da internet e com custos reduzidos.

Deste modo, deve-se levar em conta a segurança da informação que transita pela *internet* visto que, por exemplo, se um *site* de comércio eletrónico não estiver seguro há sempre o risco de, quer o comprador como o vendedor, perder sem poder efetuar a sua compra.

Consequentemente, a presente monografia intitulada "Segurança do Comércio Eletrónico – O caso de Cabo Verde" realça o comércio eletrónico, a segurança da informação bem como um caso prático onde foi aplicado os conceitos dos conteúdos teóricos para o caso de Cabo Verde sem deixar de lado a análise efetuada a alguns *sites* de comércio eletrónico em Cabo Verde.

Abstract

With the need to expand the business along with the expansion of the Internet and the emergence of new technologies, e-commerce whose aim is to facilitate the process of buying and selling without the need for construction of new facilities since emerged that it can be expanded to worldwide via the internet and with reduced costs.

Thus, one should take into account the security of information, via the internet since, for example, if an e-commerce site is not safe there is always the risk of both buyer and seller, without losing power to perform your purchase.

Consequently, this monograph entitled "Segurança do Comércio Eletrónico – O caso de Cabo Verde" enhances e-commerce, information security as well as a case where the concepts of the theoretical contents in case of Cape Verde was applied without neglecting the examination of some e-commerce sites in Cape Verde.

Agradecimentos

Primeiramente agradeço a Deus pela dádiva da vida, força, saúde e paz durante a minha caminhada enquanto estudante da Universidade Jean Piaget de Cabo Verde.

Agradeço a minha família que me tem apoiado incondicionalmente em todos os momentos da minha vida, a minha filha que tem sido a minha fonte de força e inspiração, aos meus amigos, colegas de curso e professores durante essa jornada e um especial agradecimento para a minha orientadora Emília Monteiro Tavares que tem disponibilizado o seu valioso tempo por me orientar durante toda a elaboração desse trabalho científico e todos que, de alguma maneira, estiveram sempre do meu lado.

Conteúdo

Tabelas

Figuras

Siglas e Acrónimos

3G *Third Generation*

ACL *Access Control Lists*

ADSL *Asymmetric Digital Subscriber Line*

ALE *Anual Loss Exposure*

ANAC Agência Nacional das Comunicações

API *Application Programming Interface*

ATM *Automatic Teller Machine*

B2B *Business-to-business*

B2C *Business-to-consumer*

BAI Banco Angolano de Investimentos

BCA Banco Comercial do Atlântico

BI Banco Interatlântico

C2C *Consumer-to-consumer*

CECV Caixa Económica de Cabo Verde

CMP Câmara Municipal da Praia

CSRF *Cross Site Request Forgery*

E-SCM *Electronic Supply Chain Management*

E-CRM *Electronic Customer Relationship Management*

EDI *Electronic Data Interchange*

GPRS *General Packet Radio Service*

HDIS *Host Based IDS*

HTTP *Hypertext Transfer Protocol*

HTTPS *HyperText Transfer Protocol Secure*

IC Infra-estrutura de Chaves Públicas

IDS *Intrusion Detection System*

IP *Internet Protocol*

IPSEC *IP Security Protocol*

ISP *Internet Service Provider*

LAN *Local Area Network*

MRO Manutenção, Reparo e Operações

NIDS *Network Based IDS*

POS *Point of Service / Point of Sale*

S/MINE *Secure Multipurpose Internet Mail Exchange*

SET *Security Electronic Transaction*

SISP Sociedade Interbancária e Sistemas de Pagamentos

SQL *Structured Query Language*

SSL *Secure Sockets Layer*

SWOT Strengths, Weaknesses, Opportunities and Threats

TEF Transferências Eletrónicas de Fundos

TACV Transportes Aéreos de Cabo Verde

TI Tecnologias de Informação

TIC Tecnologias de Informação e Telecomunicação

URL *Uniform Resource Locator*

VPN *Virtual Private Network*

XSS *Cross Site Scripting*

Introdução

Com o aumento das Tecnologias de Informação e Telecomunicação (TIC) nos diversos ramos de atividades, surgiu-se a necessidade por parte das entidades que fornecem produtos e serviços de facultarem aos seus clientes uma forma de ver e comprar os seus produtos sem estarem presencialmente na loja, podendo os mesmos estarem geograficamente distantes.

Deste modo é que surge uma nova abordagem denominada de comércio eletrónico que, não só, é uma nova forma de comprar produtos/serviços como também uma forma de expandir o negócio tanto a nível nacional como a nível internacional.

Cabo Verde surge nesse contexto de avançar a nível das tecnologias da informação adotando essa nova abordagem, embora ainda numa fase inicial tendo em conta que recentemente o comércio eletrónico começou a operar aqui no país.

Ao longo deste trabalho será abordado os conceitos de comércio eletrónico, da segurança informática, bem como o comércio eletrónico em Cabo Verde onde serão analisados, utilizando a ferramenta *Acunetix v8.0,* as vulnerabilidades nos *sites* de comércio eletrónico em e as recomendações para a resolução das vulnerabilidades encontradas.

1 Justificativa

O tema do presente trabalho foi escolhido tendo em conta a aderência que o mundo todo tem quanto a essa nova abordagem que é o comércio eletrónico.

Tendo em conta que comércio eletrónico visa transações comerciais utilizando a *internet* entre outras plataformas, também surge a necessidade de abordar a segurança nessa matéria visto que todos buscam, nos seus negócios, a transparência e o bem-estar do cliente.

2 Objetivos

- Geral:
    - Expor as principais especificidades do comércio eletrónico e da segurança que acarreta, bem como a realidade Cabo-Verdiana na matéria.
- Específico:
    - Apresentar os principais conceitos, mecanismos e técnicas do comércio eletrónico.
    - Expor os requisitos e técnicas para a segurança eletrónica no comércio eletrónico.
    - Analisar o nível de segurança informática nos *sites* de comércio eletrónico em Cabo Verde.

3 Metodologia

Para a elaboração do presente trabalho científico, as metodologias utilizadas são as seguintes:

- Pesquisas bibliográficas:
    - Livros;
    - Artigos científicos.
- Análise dos *sites* de comércio eletrónico em Cabo Verde, recorrendo à utilização da ferramenta *Acunetix v8.0*, para a recolha de possíveis vulnerabilidades existentes.

4 Estrutura do trabalho

O presente trabalho científico está estruturado em três grandes capítulos, sendo eles:

- **Segurança Informática**: onde serão abordados os conceitos relacionados com a segurança informática bem como os tipos de ataques existentes e as formas de prevenir tais ataques, realçando o valor da informação enquanto ativo importante de

qualquer sistema de informação bem como a sua devida utilização a ponto de extrair o maior proveito da mesma bem como protege-la contra possíveis ataques.

- **Comércio Eletrónico**: onde serão abordados os conceitos relacionados com o comércio eletrónico, bem como as vantagens e desvantagens dessa nova abordagem e também com o foco principal na segurança do comércio eletrónico, realçando a importância do surgimento desse fenómeno na evolução dos negócios que anteriormente funcionavam basicamente pelo comércio tradicional.
- **Segurança do Comércio Eletrónico em Cabo Verde**: onde será feita a análise dos *sites* de comércio eletrónico em Cabo Verde bem como compreender o nível de segurança informática no comércio eletrónico em Cabo Verde, realçando o seu percurso em Cabo Verde desde o surgimento da *internet* em 1997 no país até ao aproveitamento dessa tecnologia para a prática do comércio eletrónico.

Capítulo 1: Segurança Informática

No presente capítulo serão abortados temas referentes à segurança da informação onde será realçado o valor da informação, enquanto ativo importante de qualquer sistema de informação, bem como a sua devida utilização a ponto de extrair o maior proveito da mesma como também protege-la contra possíveis ataques.

1 Importância da informação

De acordo com Rezende e Abreu (2000) apud Laureano (2005), "*a informação é o dado com uma interpretação lógica ou natural dada a ele por seu usuário*". Segundo o mesmo autor, o valor da informação depende da entidade que a possui, ou seja, para alguns pode não significar nada enquanto para outros, essa mesma informação poder ser de grande importância.

"*É evidente, na atualidade, que nada poderia funcionar sem uma quantidade significativa de informação como elemento que impulsiona os fenômenos sociais e que é por eles impulsionada*" (Silva e Tomaél, 2007).

Ainda de acordo com o mesmo autor acima citado, para que a informação seja inteligentemente utilizada, é importante que a mesma seja administrada de modo que a empresa possa manter a competitividade perante as demais empresas.

Segundo Laureano (2005), ter a informação correta e no momento exato, significa tomar decisões de forma ágil e eficiente.

Sendo que a informação é um ativo muito precioso, ela dever ser gerida, diferenciada e salvaguardada para o melhor proveito da informação para a organização visto que ela é a essência da inteligência competitiva (Laureano, 2005).

1.1 Sistema de informação

Um sistema de informação é um conjunto de subsistemas interligados entre si que recolhem dados e os processa, gerando como saída informações valiosas cujo objetivo é ajudar os gerentes nas tomadas de decisões, a apoiarem a coordenação e o controlo de uma organização (Laureano, 2005).

Segundo o mesmo autor, para produzir informações úteis necessárias para tomar decisões, controlar operações, analisar os problemas que vão surgindo e criar novos produtos e serviços, os dados recolhidos passam por três atividades distintas, sendo elas a entrada, o processamento e a saída.

De acordo com Silva e Tomaél (2007), tudo que, direta ou indiretamente, influência a informação deverá ser identificado de modo que se possa precaver as influências que poderão surgir durante o processo bem como detetar possíveis problemas durante o fluxo da informação.

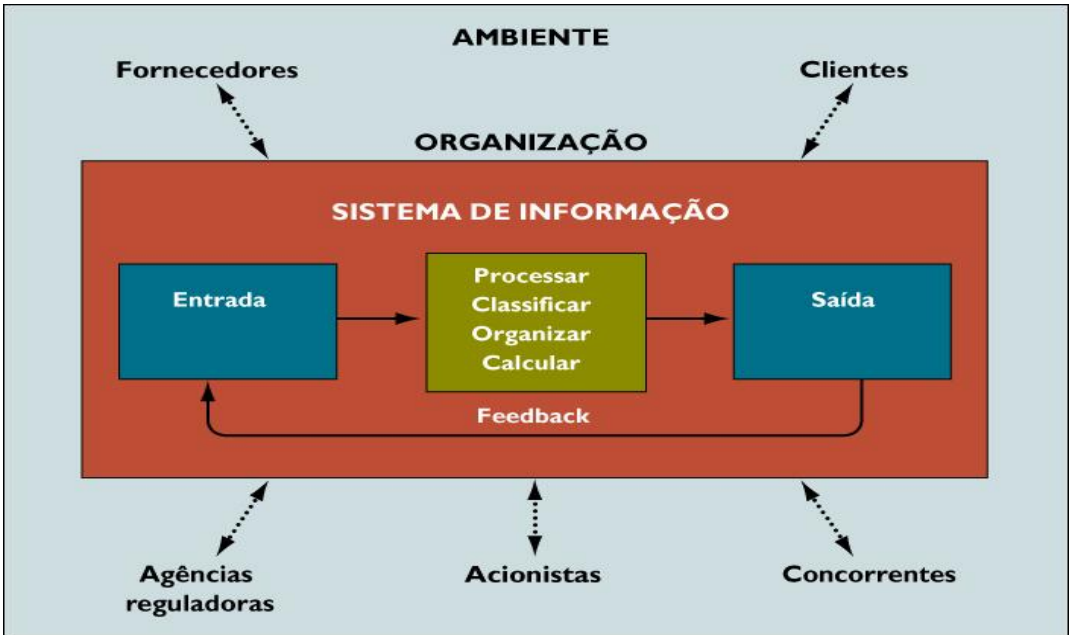

Figura 1 – Sistema de informação
Fonte - Laureano (2005)

A entrada dos dados tem a ver com recolha de dados que podem ou não ser importantes à empresa. O processamento trata os dados no seu estado bruto produzindo informações, sendo que nesta fase são eliminados os dados que não trazem valor significativo à empresa. A saída surge quando os mesmo já se encontram devidamente tratados e que já possuem um valor para a organização, sendo que o mesmo é utilizada por pessoas e/ou atividades. E por fim tem-se o *feedback* onde as informações produzidas pela organização são submetidas a avaliações, podendo provocar alterações no processo de recolha de dados, ou seja, na entrada.

Um sistema de informação surge como um ativo de extrema importância para o sucesso de qualquer organização, visto que ele dita as regras do negócio.

1.2 Classificação das informações

Segundo Laureano (2005), apesar de as informações serem importantes para a organização, nem todas merecem cuidados especiais.

De acordo com Reis et all, para a classificação das informações, há que se levar em consideração os seguintes aspetos para que a mesma seja examinada:

- Integridade – onde é analisada se a informação é atual, completa e administradas por pessoas autorizadas.
- Disponibilidade – onde é analisada se a informação encontra-se sempre disponível/acessível quando a mesma eh necessária.
- Confidencialidade – onde a informação, somente, é acedida por pessoas devidamente autorizadas.
- Valor – onde é verificada se a informação possui um grande valor para a organização que a mantém.

1.3 Ciclo de vida das informações

De acordo com Choo (2003) apud de Paula (2011), a informação atravessa por um processo contínuo sendo que, a cada fase, a mesma deverá ser monitorada.

A figura abaixo mostra todos os momentos que a informação atravessa até que a mesma seja utilizada:

Figura 2 – Atividades da gestão da informação
Fonte – de Paula (2011)

Sendo que, de acordo com o mesmo autor, as fases ou momentos são definidas da seguinte forma:

- Identificação das necessidades: processo onde é identificada o quão relevante é a informação para os processos estratégicos.
- Obtenção: processo onde são recolhidos e classificados os dados.
- Organização e processamento: processo onde pelos qual os dados são processados, examinados, classificados e interpretados de modo que os mesmos possam ser tratados e organizados em diferentes formatos e suportes.
- Armazenamento: processo onde, após a organização e processamento, as informações são guardadas mediante o conteúdo das mesmas.
- Disseminação: processo onde a informação é divulgada pelas pessoas que a necessitam, divulgação essa que pode ser de maneira formal ou informal.
- Utilização: processo onde as informações são aproveitadas, para utilização ou análise, pelo pessoal da organização.
- Realimentação: processo pelo qual onde são reconhecidas novas necessidades a partir do conhecimento produzido e onde o ciclo é reiniciado.

2 Segurança da informação e seus critérios

De acordo com TCU (2008), "*a segurança de informações visa garantir a integridade, confidencialidade, autenticidade e disponibilidade das informações processadas pela organização*":

- Integridade: baseia-se na fiabilidade das informações. Verifica a coerência dos dados depositados relativamente às inserções, alterações e processamentos autorizados. Também, verifica a coerência dos dados enviados pelo emissor com os recebidos pelo

recetor. Basicamente, a integridade garante a não-violação dos dados, seja ela acidental ou propositada.

- Confidencialidade: baseia-se na garantia de que somente pessoas devidamente autorizadas tenham acesso às informações armazenadas. Deste modo, evita-se que pessoas não autorizadas tenham acesso à essas informações, de forma acidental ou propositada.
- Autenticidade: baseia-se na garantia da veracidade da fonte das informações bem como na confirmação da identidade da pessoa que disponibiliza a mesma.
- Disponibilidade: baseia-se na garantia de que a informação está sempre acessível as pessoas devidamente autorizadas sem que haja interrupções no entrega da informação para quem de direito.

3 Gestão do risco

De acordo com Silva *et all* (2003), gestão de risco é o processo de identificação de medidas de segurança de modo a garantir o nível de segurança á empresa desejado a sua administração.

Este processo é constituído por uma sequência de fases onde os riscos são identificados, determinados e classificados que posteriormente são estabelecidos um conjunto de medidas de segurança permitindo, deste modo, a minimização ou eliminação dos riscos que a empresa se encontra sujeita.

As fases do processo de gestão do risco são segundo o mesmo autor acima supracitado:

- Identificação dos riscos;
- Análise de risco;
- Identificação de controlos (medidas de segurança);
- Seleção de controlos ou medidas de segurança.

3.1 Identificação dos riscos

A identificação dos riscos é o primeiro processo na gestão do risco visto que a mesma faz o levantamento de todos os riscos mediante a área de atuação da empresa (Silva et all (2003)).

Ainda continuando com Silva *et all* (2003), para se determinar o contexto da empresa, poderão/deverão ser levados em conta os seguintes modelos:

- *SWOT*: baseia-se na relação entre a empresa e o ambiente em que se encontra inserido mediante a identificação de pontos fortes, fracos, ameaças e oportunidades que a emprese se encontra sujeita.
- Contexto: baseia-se na descrição da empresa mediante a identificação das suas capacidades, metas, objetivos e estratégias adotadas para os alcançar.
- Alvo: baseia-se na descrição das metas e objetivos, estratégias, âmbito e parâmetros da gestão de riscos.
- Bens: baseia-se na descrição dos bens da empresa e das suas interdependências.

Após a determinação do contexto da empresa e contextualizado o cenário de risco em que a empresa se encontra presente, poder-se-á identificar os elementos necessários para a análise de risco.

3.1.1 Ameaças

Segundo Laureano (2005), a ameaça pode ser definida como "*qualquer acão, acontecimento ou entidade que possa agir sobre um ativo, processo ou pessoa, através de uma vulnerabilidade e consequentemente gerando um determinado impacto. As ameaças apenas existem se houverem vulnerabilidades, sozinhas pouco fazem*".

De acordo com Sêmola (2003) apud Laureano (2005), as ameaças podem ser divididas tendo em conta a sua intencionalidade e separadas por grupos:

- Naturais – baseiam-se em ameaças provenientes de fenómenos naturais, tais como terramotos, tempestades, incêndios naturais, etc.
- Involuntárias – baseiam-se em ameaças provenientes de ações humanas de forma involuntária, na maioria das vezes causadas pelo desconhecimento ou descuidos, tais como acidentes, erros, falta de energia, etc.
- Voluntárias – baseiam-se em ameaças provocadas por ações humanas de forma propositada, feitas pelos invasores, espiões, ladrões, etc.

3.1.2 Ataques

"*O ataque é o ato de tentar desviar dos controles de segurança de um sistema de forma a quebrar os princípios citados anteriormente*" (Laureano, 2005).

De acordo com o mesmo autor, para a implementação de medidas de segurança, torna-se necessário classificar as possíveis formas de ataques em sistemas:

- Interceção – baseia-se no acesso a informações por pessoas não autorizadas.
- Interrupção – baseia-se na interrupção do fluxo normal das mensagens da origem até ao destino.
- Modificação – baseia-se na modificação ou transformação por pessoas não autorizadas, violando, deste modo, a integridade da mensagem.
- Personificação – baseia-se no acesso não autorizado de pessoas que enviam mensagens fazendo-se passar por uma pessoa autêntica e autorizada.

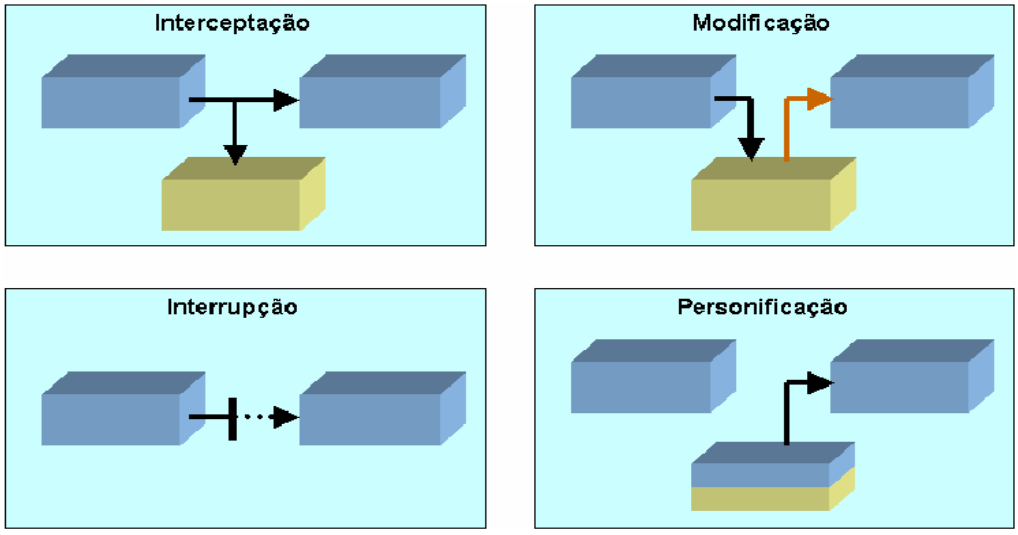

Figura 3 – Formas de ataque
Fonte - Laureano (2005)

Segundo OWASP (2007), dentre as vulnerabilidades mais exploradas pelos *hackers* baseiam-se em:

- *SQL Injection*:

- Definição: Consiste na inserção de dados em forma de comandos *SQL* por parte do *hacker* com o intuito de aproveitar de forma indevida de dados ou informações.
- Proteção:
  - Validação de entradas;
  - Utilização de *API* segura;
  - Evitar mensagens detalhadas de erros;
  - Evitar privilégios altos ao conectar à base de dados;
  - Entre outras.

- *Cross Site Scripting* (*XSS*):
  - Definição: Consiste na inserção de *scripts* nas páginas *Web* com o objetivo de roubar sessões do utilizador, modificar/desfigurar *sites*, inserir conteúdos ofensivos, roubar informações pessoais, entre outras.
  - Proteção:
    - Validação de entrada;
    - Conversão de caracteres do tipo de *script* para caracteres inofensivos;
    - Codificação na saída de dados;
    - Entre outras.

- *Cross Site Request Forgery* (*CSRF*):
  - Definição: Consiste no envio de uma requisição, por parte de um utilizador autenticado, para uma aplicação *Web* vulnerável de forma forçada com o objetivo de fazer-se passar pelo referido utilizador autenticado de modo a realizar ações em nome da vítima.
  - Proteção:
    - Não utilizar requisições *GET* (*URLs*) para dados sensíveis;
    - Para dados sensíveis/transacionais, re-autenticar ou utilizar assinaturas de transação;
    - Garantir que não haja *Cross Site Scripting* (*XSS*);

- Entre outras.

3.1.3 Vulnerabilidades

De acordo com Silva *et all* (2003), a identificação das vulnerabilidades permite calcular a probabilidade da realização das ameaças à empresa.

"*Todos os ambientes são vulneráveis, partindo do princípio de que não existem ambientes totalmente seguros. Muitas vezes encontramos vulnerabilidades nas medidas implementadas pela empresa*" (Laureano, 2005).

Laureano (2005), ainda diz que a identificação das vulnerabilidades que podem por em risco a empresa ajuda e muito na identificação de medidas de segurança adequadas.

A figura 5 abaixo mostra que as vulnerabilidades são as principais causas de ocorrências de incidentes de segurança.

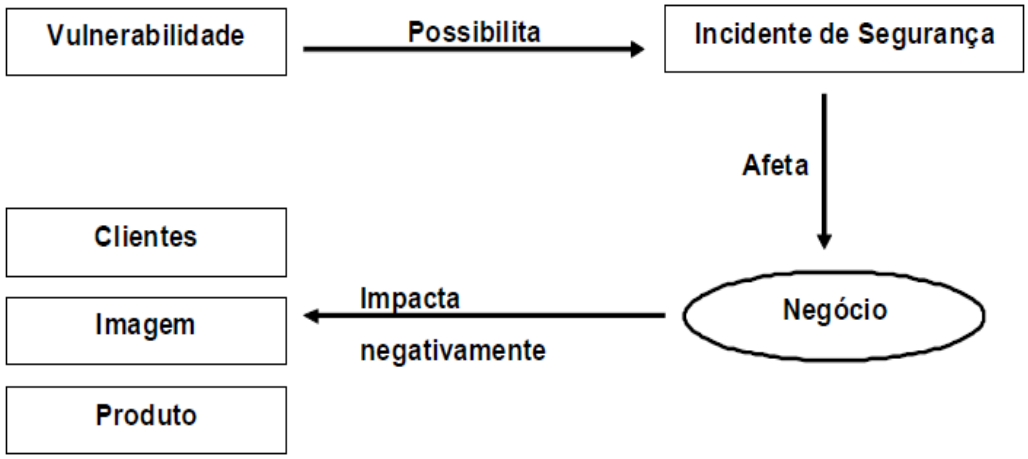

Figura 4 – Efeito da vulnerabilidade
Fonte - Laureano (2005)

3.1.4 Bens

Para a análise quantitativa do risco é necessária a identificação dos bens em que a medição dos riscos é feita através do impacto resultante da realização da ameaça (Silva *et all*, 2003).

"*A principal dificuldade na identificação dos bens, bem como na estimativa dos danos, regista-se relativamente aos bens intangíveis, uma vez que o seu carácter subjetivo dificulta a definição de modelos e métricas*", Silva *et all* (2003), ou seja, se um bem, podendo este ser um computador, for danificado, o mesmo terá um custo calculável para a sua substituição, enquanto se a imagem da empresa for afetada, será difícil quantificar as perdas.

3.2 Análise de risco e de impacto

A análise de risco permite a empresa analisar o grau de exposição de todos os possíveis acontecimentos perigosos que a empresa se encontra sujeita. Após a identificação pormenorizada das ameaças, vulnerabilidades e bens, a análise de risco encarregar-se-á na caracterização dos riscos, tanto a nível qualitativo como quantitativo, da probabilidade da concretização das ameaças e os possíveis danos que poderão ser causados caso tais ameaças concretizarem (Silva *et all*, 2003).

Para o mesmo autor, o outro tipo de análise é a de impacto onde são determinados quais as atividades fundamentais pela sobrevivência da empresa no caso da concretização de uma catástrofe.

3.2.1 Análise de risco quantitativa

De acordo com Silva *et all* (2003), para este tipo de análise pode-se utilizar a Exposição Anual à Perda (ou *Anual Loss Exposure - ALE*) onde pode-se estimar, caso a ameaça ocorrer, o valor da perda estimável.

Para estimar essa análise, é preciso recorrer às seguintes fórmulas:

ALE = Valor x R

R = V x P

Onde:

ALE é a perda monetária de ema empresa;

Valor é o valor acumulado pela concretização das ameaças;

R é a probabilidade da ocorrência de ameaças na empresa no período de um ano;

V é o valor atribuído a vulnerabilidade da empresa à ameaça:

V = 0, empresa invulnerável à ameaça;

V = 1, empresa com exposição à ameaça normal;

V > 1, empresa com exposição à ameaça superior ao normal;

P é a probabilidade, expressa em número, esperada que a ameaça se concretize por ano na empresa:

P = 1, concretização da ameaça é de uma vez por ano;

P = 0.1, concretização da ameaça é de uma vez por década;

P = 12, concretização da ameaça é de uma vez por mês;

3.2.2 Análise de risco qualitativa

Feita a identificação dos riscos que a empresa está sujeita, a análise de risco qualitativa baseia-se na avaliação do impacto e da probabilidade desses riscos priorizando-os de acordo com os efeitos dos mesmos.

Segundo Silva *et all* (2003), a análise de risco qualitativa baseia-se em quatro fases:

- Constituição da equipa;
- Realização de sessões de classificação das ameaças;
- Realização de sessões de classificação dos impactos;
- Cálculo dos riscos.

A constituição da equipa é considerada, pelo mesmo autor, como fundamental e preponderante para o resultado no final da análise de risco qualitativa visto que o responsável pela segurança terá o papel de escolher pessoas competentes a fim de ter a melhor análise e consequentemente a melhor solução.

Tendo a equipa completa, serão realizadas sessões de classificação das ameaças e dos impactos onde os membros da equipa classificarão, através de valores, as ameaças para o grau de probabilidade e de impacto de cada ameaça.

Após as sessões de classificação das ameaças e dos impactos, será feito o cálculo do risco relacionando a probabilidade e o impacto apurado pelos membros.

Ameaça	Probabilidade	Impacto	Risco
Incêndio	1	5	
Inundação	2	1	
Furto	2	2	
...	...	...	

Tabela 1 – Ficha de classificação das ameaças
Fonte - Silva *et all* (2003)

De acordo com o mesmo autor, após o apuramento das classificações das ameaças e dos impactos por parte dos membros das equipas, o risco é calculado através da seguinte fórmula:

- Risco = Probabilidade + Impacto

3.2.3 Análise de Impacto no Negócio

"*A análise de impacto no negócio visa apurar quais as funções, processos e atividades de suporte (tecnológicas ou não) críticas para o funcionamento da empresa*, ou seja, toda e qualquer tarefa realizada na empresa é essencial, independentemente das outras, mas existem tarefas das quais são consideradas críticas para o funcionamento da empresa, portanto, para tais tarefas, serão garantidos os respetivos funcionamentos para que a empresa possa operar minimamente em caso de desastre (Silva *et all*, 2003).

De acordo com o mesmo autor, não existe atividade, funções ou processos não críticos, visto que a própria existência permite denotar a sua necessidade para o funcionamento da empresa, mas existem atividade, funções ou processos que poderá dificultar a viabilidade da empresa no caso das mesmas estiverem indisponíveis durante um certo período de tempo, ou seja, existem aquelas que contribuem de maior ou menor forma para o funcionamento da empresa, e são essa as que serão preservadas em caso de desastre/catástrofe. "*Ao classificar uma função como "crítica" estaremos, na realidade, a indicar que a tolerância da empresa à sua indisponibilidade é menor que o tempo necessário a recuperação dessa função sem recurso a mecanismos de proteção contra desastre*" (Silva *et all*, 2003).

3.3 Estratégia de controlo

Após o levantamento de todos os eventuais risco e dos impactos causados pelos mesmos riscos, torna-se necessário estabelecer padrões que deverão ser colocadas em prática de modo a aumentar a segurança. Para permitir a minimização dos efeitos causados, no caso da concretização dos riscos, é necessário identificar e selecionar os processos minimizando, deste modo, os danos causados através da concretização dos riscos (Silva *et all*, 2003).

3.3.1 Arquitectura

Segundo Silva *et all* (2003), "*A definição da arquitetura alvo para a segurança dos sistemas de informação, assente numa estratégia global, irá permitir que as diversas intervenções, mesmo que pontuais, sejam consistentes com os objetivos definidos da segurança e*

contribuam para aumentar a sua maturidade", porém, na minoria dos casos, a definição ou conceção de sistema de informação é feita tendo em conta uma estratégia para a segurança da mesma, sendo que na maior parte das vezes, o responsável pela segurança do sistema de informação é contratado quando o mesmo já se encontra em produção pelo que é mais provável que haja revolução no sistema de informação do que propriamente a sua evolução.

A definição da arquitetura de segurança permite que o sistema de informação mantenha, por muito tempo, a sua consistência mesmo após as intervenções pontuais nelas aplicadas.

3.3.2 Abordagens ao Controlo de Riscos

De acordo com Silva *et all* (2003), criado um mapa de risco "*será possível implementar uma estratégia para a segurança, ordenando os riscos por prioridade e identificando o controlo adequado a cada um*", auxiliando, deste modo, o tratamento dos diversos riscos que uma empresa enfrenta.

O mesmo autor revela que o mapa de risco poderá ser representado através de gráfico bidimensional em função da sua frequência de concretização (num dos eixos) e impacto (no outro eixo).

O autor exemplifica representando duas estratégias distintas baseadas em mapas de risco.

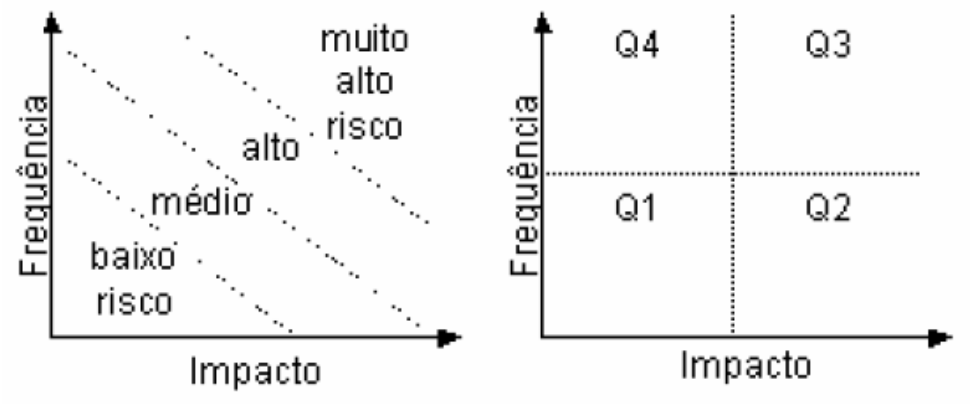

Figura 5 – Regras baseadas no mapa de risco
Fonte - Silva *et all* (2003)

A estratégia apresentada do lado esquerdo baseia-se na prioridade atribuída aos controlos pela área correspondente ao grau de risco enquanto a estratégia do lado direito baseia-se numa abordagem ao risco (evasão, redução, aceitação e transferência) em função do quadrante do mapa em que este se encontre:

- Q1 – aceitação;
- Q2 – transferência (por exemplo, seguro);
- Q3 – redução (da frequência e impacto do risco);
- Q4 – evasão (redução da frequência de concretização do risco).

3.3.3 Maturidade

Silva *et all* (2003), modelo de maturidade define os "*níveis de complexidade, em que são definidos níveis de complexidade, à semelhança dos degraus de uma escada, que deverão ser percorridos sequencialmente*", ou seja, a introdução de controlos básicos antecede a introdução dos controlos mais sofisticados.

De acordo com o mesmo autor, o modelo de maturidade baseia-se nas seguintes etapas:

- Definição de políticas e normas de segurança;
- Definição da arquitetura e dos processos da segurança;
- Implementação dos processos de suporte à inspeção, proteção, deteção e reação;
- Realização de ações de sensibilização e de formação em segurança;
- Realização periódica de auditorias e testes à segurança;
- Implementação de processos de resposta reflexa;
- Validação do modelo de proteção e da sua implementação.

De acordo com o modelo acima, as primeiras etapas baseiam-se na definição das regras/processos de segurança, de seguida iria ser implementada essas mesmas regras/processos onde seriam sensibilizados a componente humana no que diz respeito a segurança, seguidamente seria efetuados os testes necessário para as regras/processos de segurança definidos anteriormente de modo que a mesma seja validada e implementada.

3.3.4 Análise Custo/Benefício

"*A análise de custo/benefício de um controlo é realizada através da comparação direta do investimento (necessário à implementação) e do custo da sua manutenção com o valor do impacto da concretização (expectável) da ameaça associada ao controlo*" (Silva *et all*, 2003).

Segundo o mesmo autor, o cálculo do *ALE* (*Annual Loss Exposure*) permite determinar, de forma mais simples, o benefício decorrente da introdução de um determinado controlo e é calculada através das seguintes fórmulas:

$$R_b = (V\text{-}V_c) \times P$$

$$ALE_b = Valor \times R_b$$

Onde:

R_b: redução da probabilidade de concretização da ameaça na empresa no período de um ano, decorrente da introdução do controlo (expressa em ocorrências por ano).

V: número que representa a vulnerabilidade da empresa à ameaça (sem unidade).

V_c: número que representa a redução da vulnerabilidade da empresa à ameaça, após a introdução do controlo (sem unidade).

P: probabilidade correspondente ao número médio esperado de vezes que a ameaça se irá concretizar por ano (expresso em ocorrências por ano).

ALE_b: redução na perda monetária média expectável num ano, decorrente da introdução do controlo (expressa numa unidade monetária).

4 Mecanismo para Controlo de Segurança

4.1 Autenticação e autorização

Segundo Laureano (2005), a autorização baseia-se num processo em que, através das listas de controlo de acessos (*Acess Control Lists - ACL*), são definidas quais as atividades/processos que um determinado utilizador está autorizado a fazer, gerando, desta forma, os chamados perfis de acesso. Por exemplo, um colaborador de uma agência bancária que desempenha a função de caixa, no seu perfil pode fazer todas as operações de caixa mas por outro lado não poderá, por exemplo, negociar uma dívida com um determinado cliente visto que no seu perfil de acesso o mesmo não tem autorização para tal.

Para o mesmo autor, uma outra medida importante para a segurança de uma empresa é a autenticação visto que a mesma poderá afirmar se de facto a pessoa é realmente quem afirma ser. Atualmente, os procedimentos de autenticação baseiam-se em três métodos distintos (Laureano (2005)):

- Identificação positiva (o que você sabe): identificação em que o requerente demonstra o conhecimento de alguma informação necessária para a autenticação, por exemplo uma senha.

Figura 6 - Identificação positiva
Fonte - Laureano (2005)

- Identificação proprietária (o que você tem): identificação na qual o requerente mostra possuir algo necessário para a autenticação, como por exemplo um cartão magnético.

Figura 7 - Identificação proprietária
Fonte - Laureano (2005)

- Identificação biométrica (o que você é): identificação na qual o requerente mostra alguma característica própria que seja necessária para o processo de autenticação, como por exemplo a sua impressão digital.

Figura 8 - Identificação biométrica
Fonte - Laureano (2005)

4.2 Combate a ataques e invasões

Para Laureano (2005), à medida que as conexões eletrónicas e as tentativas de acesso indevido aumentam, torna-se necessário proteger um dos bens mais valioso da empresa, a informação, quer com dispositivos de hardware e software de proteção, quer com o controlo de acessos e naturalmente combate a ataques e invasões.

4.2.1 Firewall

Tendo em conta Laureano (2005), *firewall* "*é um sistema (ou grupo de sistemas) que reforçam a norma de segurança entre uma rede interna segura e uma rede não-confiável como a Internet*". O *firewall* é vista como uma barreira entre a rede interna e a rede externa onde só deixa passar, de uma rede para a outra, dados que previamente foram definidos pelo administrador de rede.

O mesmo autor realça que um *firewall* tem a função de proteger as fontes de informação de uma empresa, mediante o controlo de acesso entre a rede interna e a rede externa.
Laureano (2005), os *firewall* podem ser classificados em duas grandes classes:

- Filtros de Pacotes: os filtros de pacotes são mecanismos que, de acordo com os padrões definidos pelo administrador de rede, autorizam ou não que determinados pacotes passem pela rede. Um exemplo ilustrado, na figura abaixo, pelo mesmo autor é o *dual homed system*, ou seja, um sistema que liga a rede interna com a rede externa:

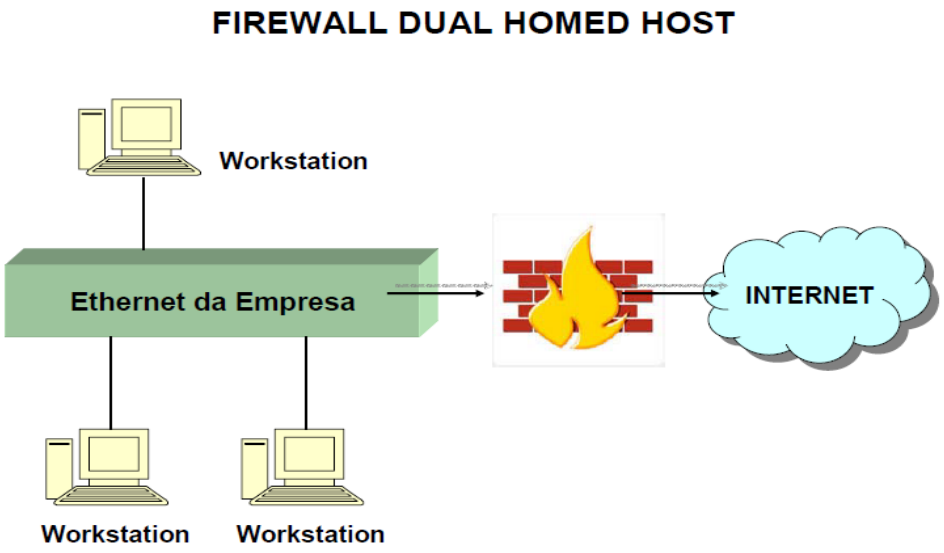

Figura 9 – Firewall *dual homed host*
Fonte - Laureano (2005)

- Servidores *Proxy*: são servidores que autorizam ou não a conexão a determinados serviços requisitados por um determinado cliente, serviços que podem ser um arquivo, uma conexão, uma determinada página *web* ou qualquer outro recurso requisitado ao servidor. O exemplo abaixo ilustra a utilização do mesmo como um elemento de aceleração de conexões em páginas *web* lentas:

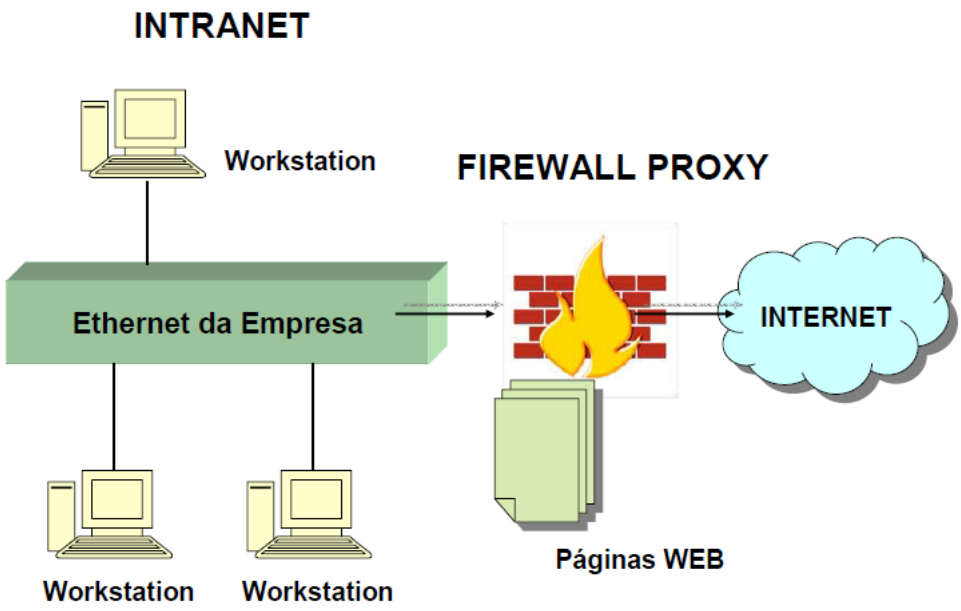

Figura 10 – Firewall *proxy*
Fonte - Laureano (2005)

4.2.2 Detector de intrusos

De acordo com Laureano (2005), o modo mais comum de detetar intrusões é através dos dados analisados pelas auditorias que por sua vez são geradas pelos próprios sistemas operacionais denominados de *logs*.

O mesmo autor relata que, atualmente, a tecnologia de deteção de intrusão (*Intrusion Detection System – IDS*) tem ajudado os administradores de segurança na detenção de intrusos através do reconhecimento de comportamentos ou ações intrusivas informando, deste modo, o administrador de segurança ou mesmo tomar, automaticamente, medidas destinadas a neutralizar tal intrusão.

"*Um IDS automatiza a tarefa de analisar da auditoria*" na visão de Laureano (2005), podendo ser usados para classificar a culpa do atacante, detetar a dimensão dos danos e antever posteriores ataques.

- Classificação de Detetores de Intrusão

Para Laureano (2005), sendo o principal objetivo da *IDS* detetar os intrusos e o uso indevido de utilizadores legítimos, esta ferramenta é executa em *background* e quando houver a deteção de algo que seja suspeita ou ilegal a mesma gera uma notificação.

Os sistemas em utilização podem ser classificados segundo Laureano (2005) em:

- Quanto à Origem dos Dados:

  Segundo o mesmo autor, existem dois tipos de implementação de ferramenta *IDS*:

  - *Host Based IDS* (*HIDS*): a instalação da mesma é feita nos servidores onde todas as informações estão contidas cujo objetivo é alertar e identificar ataques e tentativas de acesso indevido á própria máquina.
  - *Network Based IDS* (*NIDS*): a instalação é feita em máquinas cujo objetivo é identificar ataques endereçados a toda a rede, monitorizando tudo o que passa na rede da empresa.

- Quanto à Forma de Deteção:

  Algumas ferramentas *IDS* possuem, por defeito, padrões de ataques com a finalidade de detetar intrusões, tais como:

  - Deteção por assinatura: baseia-se na recolha dos dados comparando-os com uma base de registos de ataques conhecidos (assinaturas).
  - Deteção por anomalia: baseia-se na recolha de dados comparando-os com o histórico das atividades consideradas normal e tudo o que for considerado como fora do normal é tida como ameaça.
  - Deteção Híbrida: baseia-se nas duas abordagens anteriores, detetando ataques conhecidos e comportamentos anormais.

4.3 Privacidade das Comunicações

4.3.1 Criptografia

Tendo em conta Laureano (2005), "*A palavra criptografia tem origem grega (kriptos = escondido, oculto e grifo = grafia, escrita) e define a arte ou ciência de escrever em cifras ou em códigos*".

- Simétrica ou de chave privada

Os algoritmos simétricos ou de chave pública são algoritmos onde a chave utilizada para cifrar a mensagem deverá ser a mesma para decifrar a mensagem, ou seja, tanto o emissor como o recetor deverão ter conhecimento da chave secreta para que a transação possa ser efetuada. Segundo o mesmo autor, o maior problema neste tipo de algoritmo é o modo como as chaves serão entregues.

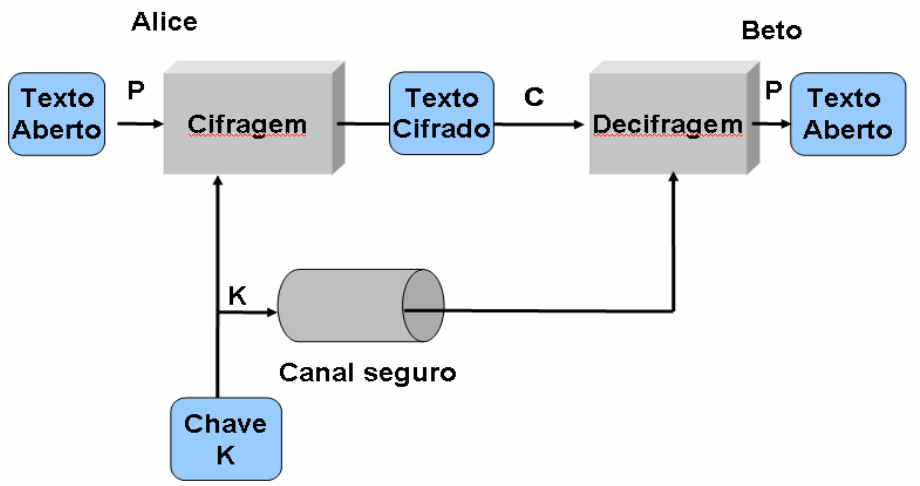

Figura 11 – Algoritmo simétrico
Fonte - Laureano (2005)

- Assimétrica ou de chave pública

  Este conceito, cujo objetivo era resolver o problema de gestão de chaves, foi introduzida em 1976 por Whitfield Diffie e Martin Hellman.

  Com este tipo de algoritmo, cada integrante possuirá um par de chaves (pública e privada), onde a chave privada é do conhecimento, exclusivamente, privado pela qual é utilizada para decifrar a mensagem recebida e a chave pública é do conhecimento público onde os outros integrante podem cifrar uma mensagem e enviá-la mas, a mesma mensagem, só poderá ser decifrada pelo proprietário da respetiva chave pública.

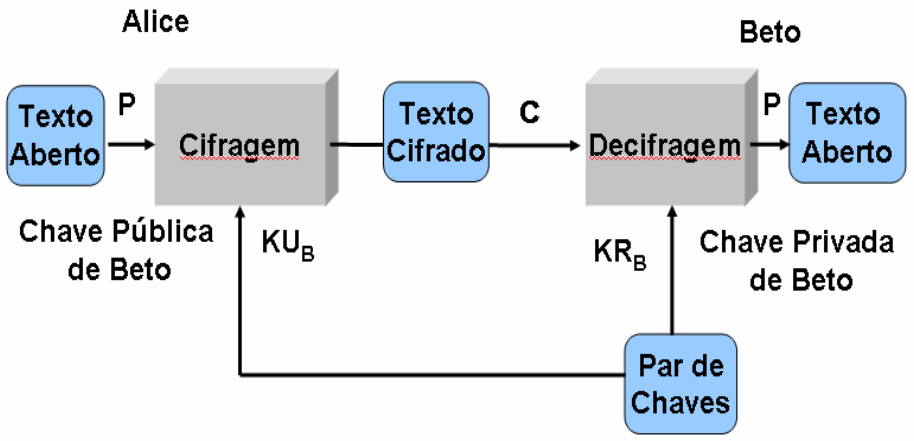

Figura 12 – Algoritmo assimétrico
Fonte - Laureano (2005)

4.3.2 Assinatura Digital

Laureano (2005) define o conceito de assinatura como sendo um processo onde apenas o signatário o possa realizar e que para a mesma possa ser considerada digital, o signatário utiliza a sua chave privada no processo de cifragem da mensagem.

O mesmo autor realça que no caso da assinatura digital não há necessidade de cifrar toda a mensagem visto que esse processo demoraria muito tempo, logo, a assinatura digital seria aplicada apenas sobre um identificador evidente do mesmo sendo que o mesmo identificador seria o resultado da aplicação de uma função *hash* onde, ao resultado da aplicação de uma função *hash*, é cifrada com a chave privada do signatário constituindo, deste modo, a assinatura digital do documento.

Tendo em conta o mesmo autor, todos podem verificar a autenticidade de uma assinatura digital através da decifração da mesma assinatura digital utilizando a chave pública do signatário, a qual todos têm acesso. Tendo verificado a autenticidade da assinatura, resta comprovar a associação da assinatura ao documento, sendo que segundo Laureano (2005) "*é feito recalculando o hash do documento recebido e comparando-o com o valor incluído na assinatura*". Feitos estes dois processos de verificação, pode-se concluir a ligação da assinatura digital com o documento, bem como a integridade do mesmo.

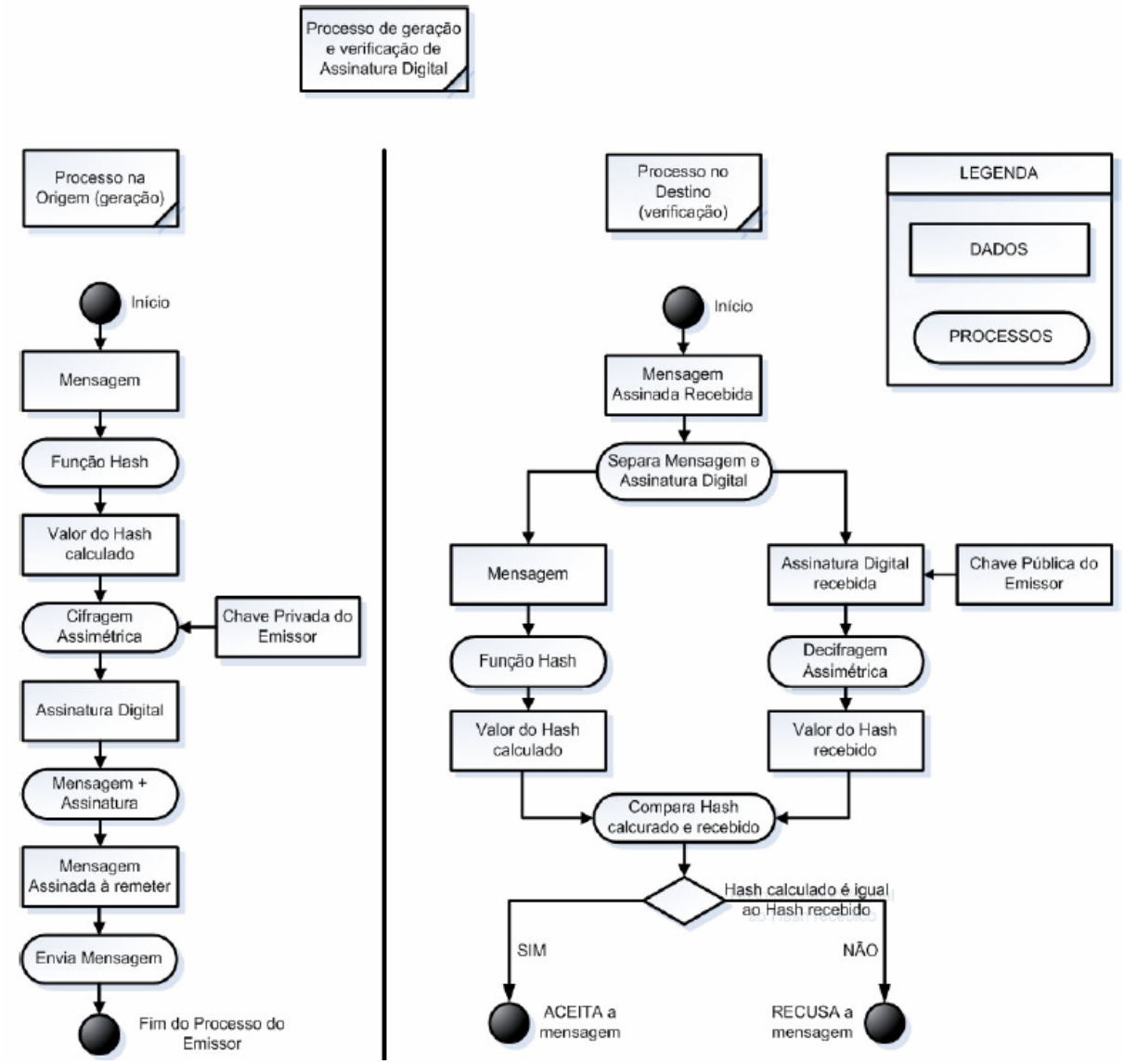

Figura 13 – Função *hash*
Fonte - Laureano (2005)

4.3.3 Virtual Private Network

Virtual Private Network (*VPN*) ou Rede Privada Virtual são, segundo Laureano (2005), "*túneis de criptografia entre pontos autorizados, criados através da internet ou outras redes públicas e/ou privadas para transferência de informações, de modo seguro, entre redes corporativas ou usuários remotos*".

O mesmo autor realça que, sendo a *internet* um meio inseguro suscetível a modificações e/ou interceções, a segurança é, não só a primeira, como a mais importante função da *VPN*.
Abaixo, estão representadas três das aplicações, consideradas importantes por Laureano (2005), para as *VPNs*:

- Acesso Remoto via *internet*: baseia-se na ligação a um provedor de acesso (*Internet Service Provider – ISP*) onde estabelece-se o acesso remoto a redes corporativas.

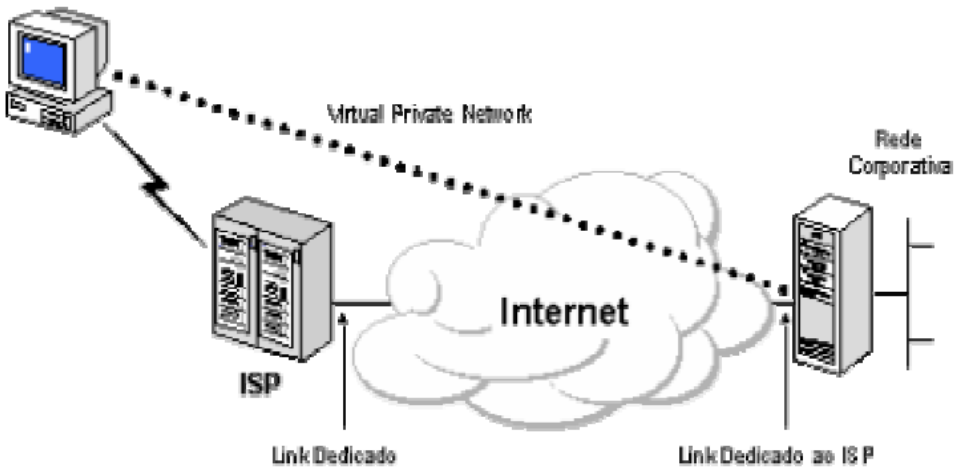

Figura 14 - Acesso Remoto via *Internet*
Fonte - Laureano (2005)

- Conexão de *LANs* via *internet*: baseia-se na criação de circuitos locais interligando-as à *internet* devendo a mesma estar disponível 24 horas por dia para eventuais tráfegos oriundas da mesma.

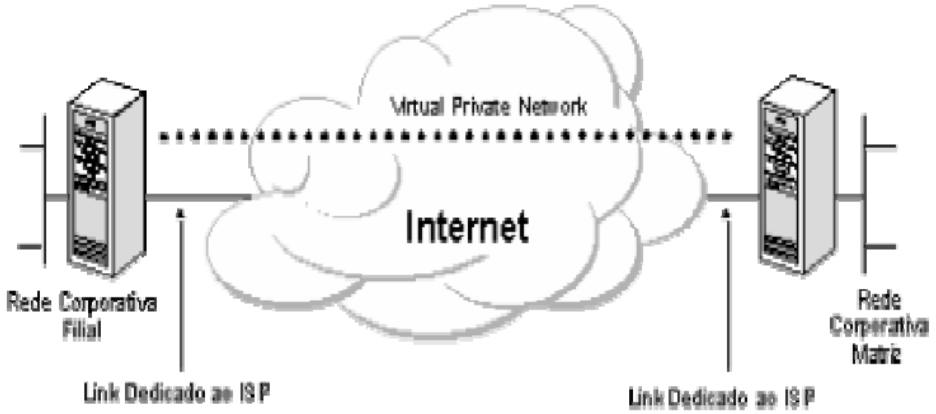

Figura 15 - Conexão de Lans via *Internet*
Fonte - Laureano (2005)

- Conexão de Computadores numa *intranet*: baseia-se na criação de uma ligação fisicamente separada da *LAN* corporativa, para um grupo restrito dentro de uma organização, onde o acesso das informações não está disponível a todos os

intervenientes da organização, garantindo deste modo, a confidencialidade das informações.

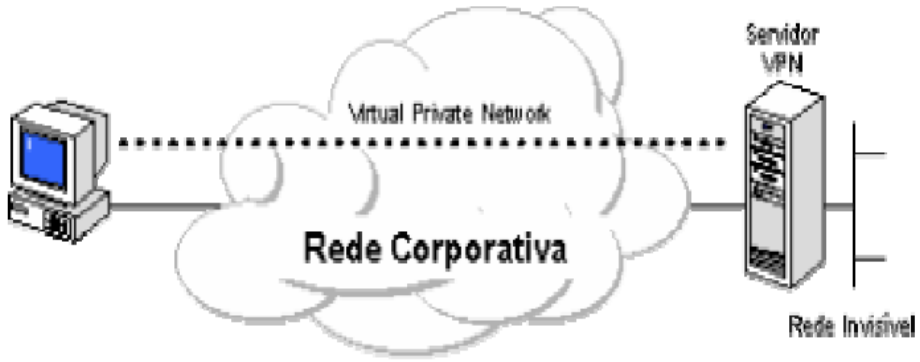

Figura 16 - Conexão de Computadores numa *intranet*
Fonte - Laureano (2005)

Sendo a *VPN* um recurso que deve permitir o acesso remoto a utilizadores autorizados aos recursos da *LAN*, a mesma deverá obedecer algumas características mínimas desejáveis numa *VPN* (Laureano (2005)):

- Autenticação de utilizadores: baseia-se na autenticação da identidade do utilizador onde somente utilizadores autorizados devem ter acesso.
- Gestão de endereços: baseia-se na atribuição de endereços fictícios do que o próprio endereço da rede privada a fim de salvaguardar o mesmo.
- Criptografia de dados: baseia-se na codificação dos dados que circulam na rede onde somente utilizadores autorizados deverão descodificar a mesma.
- Gestão de chaves: baseia-se na gestão das chaves utilizadas para descodificar a mensagem cifrada onde somente um grupo de utilizadores autorizados deverá ter acesso a mesma.
- Suporte a múltiplos protocolos: baseia-se no suporte aos diversos protocolos existentes tal como *IP* (*Internet Protocol*) para que haja tráfego de mensagens na rede pública.

4.3.4 Public Key Infrastructure

De acordo com Laureano (2005), "*uma Infraestrutura de Chaves Públicas (ICP) é um sistema de segurança baseado em tecnologia para estabelecer e garantir a confiabilidade de chaves*

públicas de criptografia" podendo a mesma contribuir para a otimização da velocidade e do valor das transações de *e-business*.

O maior objetivo dessa arquitetura moderna tem a ver, segundo Laureano (2005), com a proteção e distribuição da informação em ambientes distribuídos onde os utilizadores podem estar em locais geograficamente diferentes.

Laureano (2005) refere a Infraestrutura de Chaves Públicas (ICP) como sendo uma mistura de *software*, tecnologia de encriptação e serviços que possibilita às organizações efetuarem comunicações e transações na rede em segurança.

"*A Infraestrutura de Chaves Públicas (ICP) consegue assegurar confidencialidade, integridade e não-repúdio de uma maneira difícil de ser fraudada e que se apresenta de forma transparente para o usuário. Estes dois pontos, transparência aliada à forte base técnica de seus mecanismos, denotam o aspeto forte desta tecnologia*" Laureano (2005).

5 Segurança Face ao Desastre

Segundo Silva *et all* (2003), o processo de proteger a organização face ao desastre é uma tarefa a ser efetuada atempadamente visto que quando o desastre bate à porta o estrago já começa a fazer os seus efeitos e se a organização não se encontra protegida, os meios funcionais, materiais, humanos e logísticos ficam comprometidos o que, consequentemente, faz com que a empresa não volte à atividade após um acidente de grandes proporções.

5.1 Anatomia de um Desastre

De acordo com Silva *et all* (2003), o conceito de desastre baseia-se num evento inesperado originando perdas e dificuldades à organização, afetando, pela negativa, na capacidade da organização em executar serviços considerado, pela mesma, como essenciais.

5.1.1 Tipos de Desastre

De acordo com o mesmo autor, os desastres são provenientes de diversos fatores:

- Fenómenos naturais (ventos ciclónicos, terramotos, inundações, etc.);
- Incêndios;
- Explosões;
- Falhas de energia;

- Falhas mecânicas;
- Distúrbios sociais (tumultos, manifestações, guerras, etc.);
- Erros humanos;
- Crimes;
- Acidentes biológicos ou químicos;
- Impactos de veículos terrestres/aéreos/navais.

Silva *et all* (2003) realça que o mesmo incidente poderá ter impacto diferente de empresa para empresa e que tudo varia de acordo com a vulnerabilidade da empresa afetada que para uma empresa poderá ser apenas uma inconveniência enquanto para outro poderá ser um desastre.

"*Consoante os casos, a capacidade de recuperação, ou de alta disponibilidade, pode representar tanto uma garantia de sobrevivência como um fator de competitividade*" (Silva *et all*, 2003).

5.1.2 Cronologia

"*Nem todos os incidentes resultam num desastre: a maioria provoca apenas um pequeno período de indisponibilidade, ou seja, uma emergência*" Silva *et all* (2003). Segundo o mesmo autor, no caso de desastre, o principal e único objetivo da empresa seria reunir todos os esforços necessários para retomar todas as atividades/processos críticos o mais rapidamente possível e que só após a retomada das atividades críticas é que a empresa poderá retomar as outras atividades, voltando, deste modo, à normalidade.

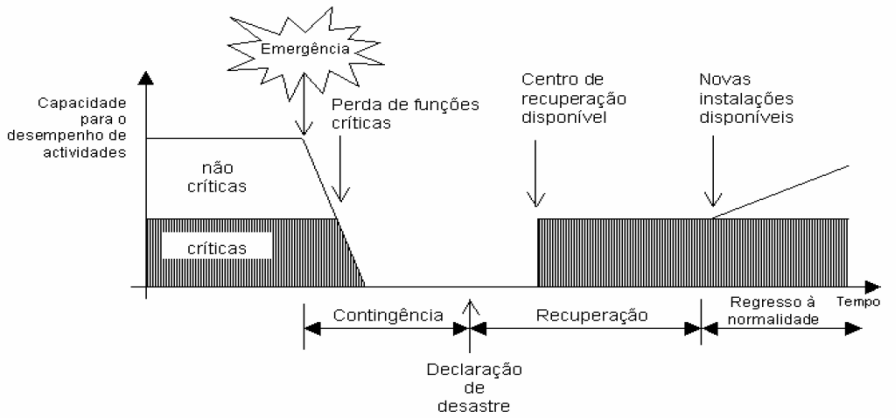

Figura 17 – Fases de um desastre
Fonte - Silva *et all* (2003)

5.2 Planeamento da Recuperação ou Continuidade do Negócio

Segundo Silva *et all* (2003), "*O projeto de planeamento da recuperação ou continuidade do negócio visa identificar as atividades a executar em caso de desastre, os responsáveis pela sua execução, os meios necessários e o modo de realização dessas atividades*".

O mesmo autor realça que o mesmo projeto é composto pelas seguintes fases:

- Arranque;
- Redução de riscos e avaliação do impacto;
- Desenvolvimento do plano;
- Implementação do plano;
- Manutenção e atualização.

5.2.1 Arranque do Projeto

Segundo Silva *et all* (2003), "*A fase de arranque do projeto de recuperação ou de continuidade do negócio é caracterizada pelo respetivo enquadramento, pela definição dos seus objetivos e âmbito, bem como pela identificação dos pressupostos e terminologia base*".

- Objetivo, Âmbito, Pressupostos e Terminologia

  De acordo com o mesmo autor, o principal objetivo do plano de recuperação de desastre ou continuidade do negócio é minimizar os estragos e consequências para um nível considerado estável para a empresa bem como reagir ao desastre.

  O mesmo autor refere ao âmbito como sendo o universo do projeto, ou seja, a definição do que é crítico para a empresa de modo a priorizá-las no que diz respeito a sua recuperação, bem como a definição das medidas de proteção a serem adotadas.

  "*Os pressupostos devem definir o cenário de desastre para o qual o plano será concebido, bem como especificar a amplitude geográfica do desastre e a dimensão ou impacto previstos sobre a Empresa e sobre a infraestrutura que a suporta (linhas de comunicação de voz e dados, pontes de energia, acessos, pessoal, etc.)* " (Silva *et all*, 2003).

- Modelo de Gestão do Projeto

A gestão do projeto de continuidade do negócio deve seguir uma estrutura bem assente de modo que os vários membros desse projeto se sinta cómodo e que, segundo Silva et all (2003), deve ser suportada por um documento que englobe:

- A descrição da atual situação da empresa em caso de proteção de desastre;
- Os objetivos, âmbito, pressupostos e terminologia;
- Os benefícios que se pretendem alcançarem com o projeto;
- A preparação das atividades de alto nível;
- A descrição da equipa que irá executar o plano;
- Os produtos finais;
- Os riscos;
- O orçamento do projeto.

5.2.2 Desenvolvimento do Plano

"*O plano de continuidade do negócio é um documento único, composto por um conjunto de outros documentos, dependendo a sua composição exata dos objetivos e âmbito definidos, bem como da estrutura precisa da Empresa e da distribuição das funções críticas no seu seio*" (Silva *et all*, 2003).

- Estratégias de Proteção

  De acordo com Silva *et all* (2003), uma estratégia de proteção baseia-se no levantamento de todos os requisitos essenciais para o normal funcionamento da empresa, onde, seguidamente serão identificadas as alternativas tendo em conta a recuperação das funções e processos essenciais da empresa.

- Plano de Contingência

  O plano de contingência é, segundo Silva *et all* (2003), um plano composto por respostas imediatas em relação a um determinado acidente onde é incluída os procedimentos de emergência bem como a descrição da equipa encarregada de executar o plano.

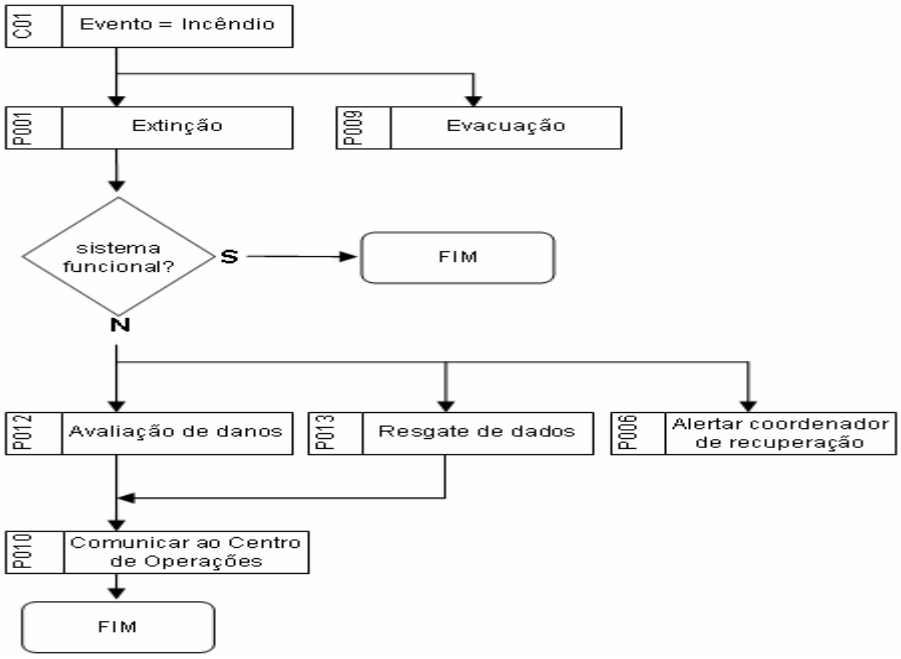

Figura 18 – Diagrama de execução
Fonte - Silva *et all* (2003)

- Plano de Recuperação

  O plano de recuperação é, segundo Silva *et all* (2003), um documento onde é descrito os procedimentos das respostas face a um incidente pelo qual impediria o normal funcionamento de atividades onde essa interrupção alargaria por um tempo superior ao estabelecido previamente.

- Plano de Regresso à Normalidade

  O plano de regresso à normalidade é, de acordo com Silva *et all* (2003), um plano onde é definida todos os procedimentos a serem levadas em conta durante a passagem das instalações de recuperação de desastre para as instalações definitivas.

- Plano de Gestão de Crise

  O plano de gestão de crise, tendo em conta Silva *et all* (2003), é um plano cuja ativação é feita por uma equipa de contingência que, durante a execução do plano de contingência, avistou com um desastre.

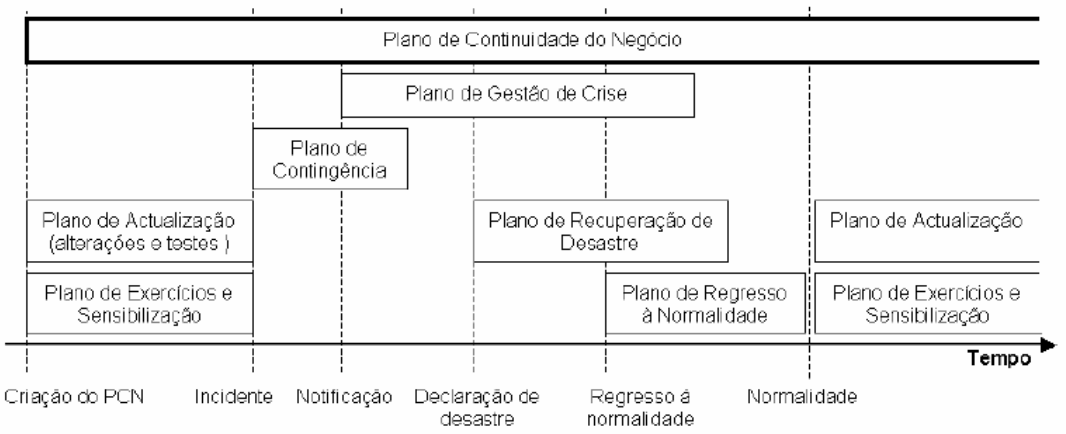

Figura 19 – Período de utilização dos planos constituintes do PCN
Fonte - Silva *et all* (2003)

- Implementação do Plano

  Após a determinação de todas as métricas a serem levadas em conta para o plano de continuidade do negócio, avança-se para a sua implementação onde é levado em conta os meios a adquirir para tal, o plano de teste bem como a sensibilização e formação onde é feita a nomeação da equipa.

- Aquisição de Meios

  De acordo com Silva *et all* (2003), o processo de aquisição de meios baseia-se na análise das diversas propostas oferecidas pelos fornecedores onde as mesmas serão sujeitas a análise e comparação entre as mesmas com o objetivo de contratar a melhor proposta.

- Plano de Testes

  O mesmo autor realça que o plano de testes tem como objetivo garantir que todos os procedimentos estabelecidos no plano de continuidade do negócio funcionam corretamente tendo em conta o retorno à normalidade da empresa em caso de desastre. Este processo permite que todos os membros da equipa saibam dos seus papéis a desempenhar e das decisões a serem tomadas em caso de desastre.

  Para Silva *et all* (2003), o plano de testes contem:

  - O processo de planeamento – baseia-se na definição do que será testado, quem irá testar, quando irá ser efetuado o teste, onde será efetuado e com que finalidade;

- O método de coordenação – tem como objetivo garantir uma articulação correta dos intervenientes do plano;
- O método de documentação – baseia-se no registo dos tempos observados, das alterações bem como da contribuição dos membros da equipa;
- O processo de avaliação e comunicação dos resultados dos testes – baseia-se na avaliação dos resultados obtidos tendo em conta o tempo alvo de recuperação e consequentemente a comunicação dos mesmos com o objetivo de sugerir melhorias, se for o caso;
- O método de inserção das modificações reconhecidas nos testes e nos procedimentos – baseia-se nas alterações verificadas durante os testes bem como às suas avaliações.

- Sensibilização e Formação

  Feito a aquisição de meios e o plano de testes, é da regra geral que todos os intervenientes do plano tenham conhecimento de todos os detalhes do plano bem como deverão saber qual a sua função dentro do plano.

  Segundo Silva *et all* (2003), "*as atividades de sensibilização permitem assegurar a comunicação do plano de continuidade do negócio a todos os intervenientes, e colaboradores em geral, dando-lhes a conhecer*":

  - Os componentes do plano;
  - A importância da proteção contra o desastre;
  - A identidade, função e contacto dos colaboradores das equipas;
  - As formas de obterem informação;
  - Em que situação é ativada o plano;
  - Quais os teste que irão realizar.

  O mesmo autor realça que além da sensibilização, atividades de formação serão necessárias para todos os intervenientes do plano cujo objetivo é dar o conhecimento procedimentos a serem tomados para que o plano de continuidade de negócio seja colocado em prática.

- Manutenção e Atualização

De acordo com Silva *et all* (2003), a manutenção e atualização do plano de continuidade do negócio obriga a implementação de um programa cujo objetivo é estabelecer uma comunicação periódica com todos os intervenientes do plano. Tal programa deve garantir permanentemente a capacidade de recuperação de desastre mediante introdução de alterações que poderão surgir.

- Plano de Exercícios e Sensibilização

  Tendo em conta o mesmo autor, "*o plano de exercícios e sensibilização irá, simplesmente, repetir ao longo do tempo o processo de realização de testes e as atividades de sensibilização/formação já abordada no âmbito da implementação do plano*".

- Plano de Atualização

  O mesmo autor, Silva *et all* (2003), realça que o plano de atualização deverá ser suficientemente consistente visto que o mesmo poderá estar sujeito a alterações do tipo de introduções de novos métodos, reformulação da mesma, reformulação da equipa afeta ao plano bem como as lições obtidas através de desastres anteriores de modo a não permitir que aconteça novamente.

Capítulo 2: Comércio Eletrónico

No presente capítulo irão ser abordados temas referentes ao comércio eletrónico bem como a importância do surgimento desse fenómeno na evolução dos negócios que anteriormente funcionavam basicamente pelo comércio tradicional.

1 Conceito

De acordo com o Dicionário do Aurélio[1], comércio [do latim *commerciu*] significa "*permutação, troca ou compra e venda de produtos ou valores; mercado negócio, tráfico*".

O comércio designa-se como uma troca, venda e compra de produtos, valores ou serviços.

Ao pensar no comércio, imediatamente pode-se realçar três diferentes papéis (Brain, 2008):

- Vendedor: aquele que disponibiliza o produto;
- Consumidor: aquele que compra o produto;
- Produtor: aquele que produz o produto, podendo, por vezes, ser o vendedor;

Então pode-se definir o comércio eletrónico como sendo uma troca, venda e compra de produtos, valores ou serviços utilizando meios/canais eletrónicos, no caso mais amplo, a *internet* mediante a utilização de um *site* (loja virtual). Neste tipo de comércio, há a exposição de produtos, valores ou serviços *online*, bem como a possibilidade de efetuar pedidos, faturação e todo o processo de transação e pagamento.

Comércio eletrónico também é conhecido como *electronic commerce* ou, de forma simplificada, *e-commerce*.

2 História da Internet

Ao falar do comércio eletrónico, de certo modo, temos que falar da *internet*.

Segundo Felz (2007), "*a internet é, de uma vez e ao mesmo tempo, um mecanismo de disseminação da informação e divulgação mundial e um meio para colaboração e interacção entra indivíduos e seus computadores, independentemente de suas localizações geográficas*".

De acordo com o mesmo autor, a *internet* representa um dos maiores sucessos de uma infraestrutura para a informação que inicialmente começaram em trocas de pacotes e que, hoje em dia, ela é uma excitante e indispensável tecnologia.

A história da *internet* é apresentada em quatro distintos aspetos de acordo com Felz (2007):

- A evolução iniciou, em 1969, com as primeiras pesquisas sobre troca de pacotes com a Arpanet e suas tecnologias.
- Os aspetos operacionais e administrativos de uma infraestrutura operacional, complexa e global.
- Os aspetos sociais que teve como resultado um elevado número de internautas que, juntos, trabalho nela de forma a evolui-la.
- O aspeto de comercialização que resulta numa infraestrutura de informação disponível e utilizável.

Nos dias de hoje, sendo a *internet* um poderoso meio de comunicação, serve como uma ferramenta ao dispor dos empresários cujos interesses são propor, ao mercado, novas formas de realização das atividades triviais no nosso quotidiano (Rocha, 2005).

3 Aparecimento do comércio eletrónico

Comércio eletrónico trata-se de um fenómeno recente muito rentável, que pode estar ao alcance de todos mas que, também, se não forem tomadas as devidas medidas de segurança pode trazer ao comerciante muitos prejuízos.

Segundo Rocha (2005), as primeiras transações do comércio eletrónico tiveram início no na década de 70 nas transferências eletrónicas de fundos (TEF), onde poderiam transferir o

[1] http://www.dicionariodoaurelio.com/, consultado a 7 de Abril de 2012

dinheiro através de meios eletrónicos, e da troca eletrónica de dados (EDI) que é uma tecnologia que, na altura, permitia a transferência de documentos por meios eletrónicos, documentos esses que podiam ser ordem de compra, faturas e pagamentos eletrónicos. Contudo, a expressão *e-commerce* só passou a ser utilizada a partir do desenvolvimento comercial da *internet*.

Devido a sua simplicidade, os internautas do mundo inteiro, de lugares geograficamente diferentes, podem comunicar-se interactivamente requisitando, deste modo, produtos e serviços. Deste modo, desde 2005, os internautas vêm acompanhando o desenvolvimento de várias ferramentas, desde os comerciais interativos até experiências em realidades virtuais (Rocha (2005)).

Segundo o mesmo autor, "*quase todas as empresas de médio e grande porte, em todo mundo, já possuem um site*".

4 A realidade do comércio eletrónico

Antigamente, expandir o negócio tinha a ver com aberturas de filiais noutros locais de forma a propagar o negócio o que envolvia a utilização de muitos recursos, nomeadamente recursos monetários, enquanto nos dias de hoje, expandir o negócio é muito mais barato do que abrir filiais noutros locais, utilizando essa nova abordagem chamada de comércio eletrónico de forma a disponibilizar o negócio ao alcance de todos tendo a *internet* como plataforma padrão.

Para Blumenschein e Freitas (2001) apud Junior (2007), o comércio eletrónico "*é realizado há mais tempo que imaginamos mesmo não estando cientes disto, pois ao fazer uma compra e efectuar o respectivo pagamento através de caixas ATM, cartão de crédito ou qualquer outro meio digital, pode-se considerar esta atividade como uma forma de comércio eletrónico*".

Muitos sectores da economia já se enquadram na realidade da utilização do comércio eletrónico como forma de se propagarem, e essa nova realidade tem vindo a crescer dia após dia, representando, desta forma, como um novo paradigma para o comércio mundial, tendo como sua grande plataforma a *internet*.

Segundo Albertin (2004) apud Cernev (2005), define o comércio eletrónico como sendo "*a transformação de toda a cadeia de valor dos processos de negócio num ambiente eletrónico, através da aplicação intensa de tecnologias de comunicação e de informação, atendendo os objetivos do negócio*".

O comércio eletrónico não só é visto como uma maneira de expandir o negócio como também uma jogada de *marketing*.

Hoje em dia, muitas empresas/lojas não possuem um edifício que pode funcionar como loja, mas sim possuem uma loja virtual (*site* na *internet*) que mostra os produtos disponíveis, podendo os clientes escolherem os produtos bem como a forma de pagamento e de entrega do mesmo. Essa nova abordagem pode ou não complementar os serviços existentes de uma loja física, podendo o comerciante ter somente um armazém onde guarda os produtos e uma loja virtual onde mostra-os e vende-os consoante os pedidos dos clientes.

A apresentação da loja virtual (*site*) deverá ser agradável, estruturada e de fácil compreensão. Só assim que se poderá distanciar-se dos concorrentes, conquistar clientes bem como manter os mesmos. Acima de tudo, todo e qualquer processo utilizado no site, ou seja, desde uma simples consulta de produtos até a compras dos mesmos deverá funcionar na perfeição para que não haja transtornos nos clientes.

Segundo Albertin (2004) apud Rocha (2005), depara que "*no comércio eletrónico, verifica-se uma nova realidade, que pode ser entendida e assimilada. Por exemplo, hoje a maior livraria do mundo, Amazon, ocupa apenas dois andares de um pequeno prédio em Seattle*", o que significa que não é obrigatório ter uma instalação física de topo para que ela possa ser reconhecida tanto a nível nacional bem como a nível mundial.

Uma das maiores dificuldades do comércio eletrónico é fazer como que o site da organização seja utilizada pelos clientes, disponibilizar tudo o que o cliente deseja ver bem como ser efetuada alguma compra utilizando a aplicação da organização.

5 Componentes fundamentais do comércio eletrónico

Todo e qualquer processo de comércio têm de haver o consumidor, o vendedor, o produto e a forma de pagamento, então, segundo dos Santos (2005), além do consumidor e do vendedor, o comércio eletrónico tem uma outra componente de extrema importância denominada de instituições bancárias que oferecem formas de pagamento do produto desejado pelo consumidor.

Quanto maior for o número de instituições bancárias associadas ao negócio do vendedor, maior serão as modalidades de pagamento que o consumidor terá a sua disposição, visto que não existe uma única instituição bancária que oferece todas as formas de pagamento possíveis.

De acordo com dos Santos (2005), estudos feitos indicam que há maior preferência de pagamento quando o mesmo for feito com cartão de crédito e/ou com boletim bancário, o primeiro é porque a maior parte dos consumidores o utilizam para os negócios *online* enquanto o segundo são para aqueles compradores que ainda não têm confiança de fazer compras *online* com os respetivos cartões de crédito.

6 Áreas fundamentais do comércio eletrónico

O comércio eletrónico utiliza diversas terminologias para a descrição de aplicações e camadas, técnicas, políticas públicas de utilização, padronização e segurança, indo da infraestrutura de rede até a estrutura de negócios e serviços. Disto, surgem diversos produtos e serviços cuja plataforma é a *internet* e o comércio eletrónico, sendo que dessas terminologias são de destacar segundo Luciano (2004) em suas pesquisas e compilado por diversos autores:

- *E-payment*: baseia-se no intercâmbio do dinheiro durante o ato da compra entre os compradores e os vendedores;
- *E-security*: trata-se das medidas de segurança necessárias para garantir que o processo da compra seja efetivado com segurança;
- *E-SCM* (*supply chain management*): baseia-se na administração da cadeia dos suprimentos de modo que os prazos da entrega dos produtos aos clientes sejam cada vez menores;
- *E-CRM*: baseia-se no processo de fornecer aos clientes um atendimento único e personalizada permitindo a maior satisfação do cliente no processo de compra.

7 Aplicações do comércio eletrónico

Inicialmente, o comércio eletrónico era utilizado unicamente para vender quando passou-se a utilizar a internet para fins comerciais. Com o aperfeiçoamento desta abordagem surgiram diferentes aplicações que podem ser utilizadas dentro do comércio eletrónico, sendo elas, de acordo com Luciano (2004):

- *E-procurement*: baseia-se num tipo de leilão onde há compra de bens e/ou serviços não-produtivos, os designados de bens MRO (Manutenção, Reparo e Operações);
- *E-learning*: também conhecido como educação á distancia, tem como objetivo fazer com que o conhecimento atinja o maior número de público-alvo sem que esta tenha que fazer esforço de se deslocar;

- *E-banking*: baseia-se numa aplicação em que clientes e bancos façam, à distância, diversas operações em suas contas mediante a utilização da *internet* e de um *browser*.
- *E-gambling*: trata-se de casinos eletrónicos em que se pode fazer apostas com cartões de crédito. A grande façanha do *e-gambling* é fazer com que, nos países onde os jogos são ilegais, os *sites* de jogos sejam armazenados nos países onde os jogos são legais sendo que os mesmos podem ser acedidos por qualquer um, independentemente da sua localização fazendo com que, deste modo, seja contornado a não legalidade dos jogos em alguns países.
- *E-auctionig*: baseia-se em leilões eletrónicos onde os participantes apresentam propostas e aquele que tiver feito a maior leva o produto/serviço.

De acordo com o mesmo autor, existem outras aplicações, de menor expressão, relacionadas com o comércio eletrónico, dentre as quais são de destacar:

- *E-directories* (catálogos eletrónicos).
- *E-franchising* (franquias eletrónicas).
- *E-trade* (compra eletrónica de ações).
- *E-engineering* (desenvolvimento colaborativo de projetos).
- *E-drugs* (farmácias online).
- Entre outras (Luciano, 2004).

8 Comércio eletrónico e o ciberespaço

De acordo com Fernandes (2000), o comércio eletrónico tem reduzido de forma drástica os investimentos no que diz respeito aos custos de instalação e manutenção que, anteriormente, as instituições comerciais e/ou industriais gastavam. Custos esses que são reduzidos principalmente quando os produtos comercializados forem digitais.

O comércio eletrónico provoca mudanças organizacionais o que influencia a economia visto que a influência das tecnologias de informação e do comércio eletrónico faz com que algumas atividades económicas sejam eliminadas enquanto aparecem outras novas.

Como consequência, as empresas que quiserem manter no mercado têm que tomar ações imediatas quanto a adoção dessa nova abordagem que é o comércio eletrónico visto que o ciberespaço está cada vez mais recetivo a estas práticas.

9 Loja Virtual

Este novo termo veio a surgir juntamente com o comércio eletrónico que, segundo dos Santos (2005), é definido como "*sites na internet, cujas páginas exibem um catálogo de produtos ou serviços que podem ser seleccionados*".

Segundo a mesma autora, no comércio tradicional, os comerciantes impunham as suas vendas em determinadas regiões e nichos económicos. E para dominar o mercado era preciso muito investimento para que o maior número de regiões seja alcançado e que, para tal, só as grandes empresas sobreviveriam.

Com o surgimento da *internet* e do comércio eletrónico, ficou facilitado para qualquer empresa que queira impor-se no competitivo mercado que existe.

Esta nova abordagem levou à criação de muitas empresas que, algumas, nem sequer possuem uma instalação física adequada para o comércio, ou seja, empresas cujo principal meio de comércio é o das lojas virtuais.

10 Oportunidades do comércio eletrónico

As tecnologias de informação vêm tendo uma influência direta no que diz respeito às mudanças nas formas de organização da produção, bem como está sendo um instrumento para o aumento da produtividade e para a competitividade dos concorrentes.

Para Tigres (1999), o comércio eletrónico é uma abordagem que utiliza a *internet*, que é uma forma menos dispendiosa, para atingir potenciais clientes finais bem como novos parceiros comerciais.

O volume das transações eletrónicas entre as empresas é muito maior do que quando o consumidor final for um cliente, visto que as empresas estão mais habituados a fazerem transações à distância, por telefone ou fax, o que implica menos resistência entre as empresas em efetuarem transações pela *internet* enquanto os clientes estão mais habituados a efetuarem transações num espaço físico.

As pequenas empresas já possuem um modo mais barato de fazer publicidade visto que o comércio eletrónico utiliza, principalmente, a *internet* como plataforma padrão o que lhes permite fazer concorrência às grandes empresas.

11 Funcionamento do comércio eletrónico

O comércio eletrónico funciona, sobretudo, à base da *internet*, onde há transferência de dados, informações, imagens entre outros, o que caracteriza a pesquisa de produtos, a escolha dos item a serem comprados, a escolha da forma de pagamento a ser adotada bem como o próprio pagamento em si.

Segundo Rocha (2005), "*entende-se por comércio eletrónico a oferta, a demanda e a contratação à distância de bens, serviços e informações, realizadas dentro de um ambiente digital, ou seja, com a utilização dos recursos típicos do que se denominou convergência tecnológica*".

O mesmo autor acima citado continua dizendo que, no que diz respeito à forma de execução, o comércio eletrónico atua-se tendo em conta duas modalidades:

- Direta: Quando há transferência de bens incorpóreos e/ou serviços utilizando o próprio ambiente virtual mediante a encomenda e o pagamento do mesmo. Os bens e/ou serviços podem ser *software*, livros ou até informações.
- Indireta: Quando não se utiliza o ambiente virtual para efetivar a transferência da encomenda por se tratar de bens corpóreos então está-se perante o comércio eletrónico indireto, visto que se utiliza outros meios para entregar a encomenda, nomeadamente os serviços de correio e/ou empresas cuja função é entregar encomendas comercializadas pela *internet*.

12 Forma de pagamento

Forma de pagamento, como o próprio nome diz, é a maneira como o cliente escolhe para pagar o seu pedido.

De acordo com Campos (2006), após escolher os produtos desejados, o cliente escolhe uma modalidade de pagamento. As modalidades de pagamento mais comum são:

- Cartão de crédito/débito: o pagamento pelo cartão de crédito é das mais fáceis e das mais utilizadas pelo consumidor. Ela consiste em fornecer o número de cartão de crédito, bem como algumas informações para verificar a veracidade do cartão de crédito bem como do titular do cartão de crédito. Este método é frequentemente utilizado em Cabo Verde.

- Boletim bancário: boletim bancário é um documento de cobrança que contém várias informações, das quais são de destacar o banco, o valor do documento, a conta pela qual se destina o valor do documento, etc., o que são importantes para o consumidor visto que ele pode imprimi-lo e pagar o valor documentado nas instalações autorizadas para tal.
- Débito em conta: esta forma de pagamento só é possível quando o consumidor é cliente do banco cuja loja onde efetua a compra também o é, visto que nesta forma de pagamento o valor da compra é descontado diretamente da conta corrente do consumidor mediante o acesso ao site do banco onde possa confirmar a compra, ou seja, o pagamento.
- Depósito ou transferência bancária: depósito ou transferência bancária é a que dá mais trabalho ao consumidor visto que o mesmo deverá anotar, para efetuar a transferência bancária, a conta, a agência e o banco da loja virtual. Seguidamente o consumidor deverá encaminhar uma cópia do comprovante de depósito à loja virtual para que o pedido possa ser entregue.
- Moeda virtual: apesar de existir outros tipos de moda virtual, o *PayPal* é dos mais conhecidos e utilizados no mundo. De acordo com o mesmo autor, *PayPal* consiste num sistema que possibilita a transferência de dinheiro entre consumidores e vendedores evitando, deste modo, a utilização dos métodos tradicionais tais como cheques, boletins bancários, ordens de pagamento, entre outros. A utilização do *PayPal* como forma de pagamento no comércio eletrónico só é possível se a loja virtual estiver possibilitada para tal.

13 Categoria do comércio eletrónico

Segundo Júnior (2007), do uso da comunicação eletrónica, aplicada aos negócios, surge três categorias básicas de comércio eletrónico, tais como de empresa-consumidor (*B2C*), a de empresa-empresa (*B2B*) e a de consumidor-consumidor (*C2C*):

- Comércio eletrónico de empresa-consumidor (*B2C*): Este tipo de comércio eletrónico baseia-se numa transação eletrónica em que um comprador/indivíduo, a partir de um computador, adquire um produto ou serviço através da *internet* efetuando, podendo ser no momento ou não, o respetivo pagamento. *B2C* são destinados aos consumidores.

Um exemplo prático é quando um indivíduo efetua uma recarga móvel utilizando uma caixa *ATM*.

- Comércio eletrónico de empresa-empresa (*B2B*): *B2B* ou comércio eletrónico entre empresas, pode ser definido como operações de compra e venda de informações, produtos e/ou serviços através da *internet* ou redes privadas partilhadas entre empresas. Um exemplo retratando esse tipo de comércio eletrónico é quando uma empresa (BCA) efetua o pagamento de consumo de água e energia elétrica a uma outra empresa (Electra).
- Comércio eletrónico de consumidor-consumidor (*C2C*): *C2C* ou comércio eletrónico entre consumidores finais, pode ser definido como operações de compra e venda de produtos entre consumidores finais.

Para este tipo de comércio eletrónico temos os leilões, onde um consumidor final disponibiliza os produtos que quer vender que será comprado por quem oferecer o maior montante num determinado prazo de tempo.

14 Razões para o investimento em comércio eletrónico

O comércio eletrónico, nos países onde a *internet* iniciou-se mais cedo, já demonstrou o seu sucesso no que diz respeito ao aumento do lucro das empresas. Essa nova abordagem está no rumo certo para se tornar cada vez mais como canal de comercialização (Felipini, 2001).

De acordo com Júnior (2007), é do conhecimento de todos que a venda de produtos por via da *internet* é uma maneira de ganhar dinheiro e como os clientes já não têm tanto receio em comprarem pela *internet*, as empresas, ou mesmo os comerciantes, podem utilizar essa nova abordagem visto que:

- O investimento é baixo.
- A empresa terá um maior alcance, alcance este que poderá ser até de nível internacional.
- Comodidade, a loja está ao alcance de todos 24 horas por dia.
- O risco de enganar o vendedor em comprar um produto e pagar depois é mínimo, ou seja, golpe.
- A assiduidade da utilização do site é enorme, visto que se o cliente gostar do *site* então voltará uma outra vez.

- Segurança, tendo em conta que o cliente pode escolher, comprar e receber o produto mesmo sem sair de casa.
- O cliente terá maior facilidade em encontrar o que procura.
- O pagamento é efetuado mediante a integração da loja com o ambiente bancário.
- O custo da manutenção é relativamente baixo.

15 Vantagens e desvantagens do comércio eletrónico

- Vantagens:

  Para Júnior (2007), são inúmeras as vantagens para a adoção do comércio eletrónico, dos quais é de realçar:

  - Maior comodidade para o cliente.
  - Segurança e pagamento dos produtos/serviços.
  - Aumento do lucro das empresas.
  - Expansão do negócio a nível global.
  - Facilidade e acesso a novos mercados e clientes.
  - Rapidez na divulgação de novos produtos e/ou promoções.
  - Etc.

A expansão do negócio é a principal vantagem do comércio eletrónico.

- Desvantagens:

  Tendo em conta o mesmo autor, as desvantagens, também, são inúmeras:

  - Fraude.
  - Aumento do número de desempregados.
  - Perda da qualidade do produto durante o ato da entrega.
  - O cliente não tem o acesso direto (contacto) com o produto antes da sua compra visto que o mesmo é visualizado através de imagens, o que pode causar algum transtorno caso o produto entregado não for o esperado.
  - Insegurança nas transações comerciais.
  - Ataques à privacidade.

- Etc.

A principal desvantagem do comércio eletrónico é a segurança, o que tem vindo a ser melhorado a fim de transmitir mais tranquilidade aos clientes quanto às transações na *internet*.

16 Segurança no Comércio Eletrónico

Segundo Campos (2006), a segurança é considerada como um dos principais, senão o principal, obstáculo ao desenvolvimento do comércio eletrónico, dada a renitência dos clientes em fornecer *online* os seus dados e em particular o número de cartão de crédito bem como o comércio eletrónico é um negócio bastante rentável o que faz com que seja alvo de ataques criminosos.

Por mais que se diga que um sistema é seguro, há sempre uma maneira de violar a sua segurança, por isso, que nenhum sistema é 100% seguro (Correia, 2010).

Apesar disto, a maioria dos especialistas argumenta que as transações são menos perigosas quando forem feitas na *internet* do que no mundo físico, dado que nos sistemas do comércio eletrónico os números dos cartões de créditos são cifrados nos servidores da empresa.

Para os comerciantes abrir uma loja virtual (*site*) é mais seguro do que abrir uma loja física, dado que se for optado pela segunda opção, esta pode ser roubada, inundada ou até ser incendiada.

Para que possa haver uma maior segurança no que diz respeito às transações comerciais, além do desenvolvimento de técnicas e tecnologias para maximizar a confiança de todo o sistema, todas as transações podem ser cifradas através da utilização do protocolo *Secure Sockets Layer* (*SSL*), protocolo esse que, atua na camada de aplicação, cria uma ligação segura ao servidor da organização protegendo (privacidade e autenticação) a informação durante a sua estadia na *internet* (Campos, 2006).

O protocolo *SSL*, que foi desenvolvido em 1994 pela *Netscape*, utiliza a criptografia da chave pública durante a transmissão dos dados podendo ser verificada nos sites em que nos *URL* dos *browsers* começa por *https* em vez de *http*. Perante este cenário pode-se dizer que o site é seguro e utiliza o protocolo *Secure Sockets Layer* (*SSL*) (Campos, 2006).

Além do protocolo *Secure Sockets Layer* (*SSL*), pode-se considerar outro protocolo de igual importância que é o *Security Electronic Transaction* (*SET*).

O protocolo *SET*, que foi desenvolvido em 1996 pelas empresas de cartões de crédito *Visa* e *Mastercard*, além de utilizar a criptografia de chave pública, ela também utiliza certificados digitais como técnicas de criptografia permitindo, desde modo, que todas as partes envolvidas no negócio se identifiquem e troquem dados/informação com segurança (Campos, 2006).

De acordo com Filho (2000) apud Correia (2010), antes de tomar por em prática qualquer medida de segurança, é preciso fazer o levantamento dos principais tipos de ameaças que possam existir. Essas medidas são para maximizar a segurança nas transações *online* e também para aumentar a confiança dos clientes/compradores.

16.1 Ameaças de segurança

Os tipos de ameaça no comércio eletrónico enquadram-se em seis grupos (Filho (2000) apud Correia (2010):

- Acesso não autorizado: este tipo de ameaça baseia-se no acesso ilegal e/ou abuso que causa danos relevantes mediante a utilização de um sistema informático.
- Alteração de dados: baseia-se na alteração de dados durante o ato da transação, tais dados que podem ser a quantidade envolvida na transação, o valor, entre outros.
- Monitorização: consiste na espionagem de dados/informações confidenciais trocadas durante o ato da transação.
- *Spoofing*: baseia-se na construção de um *site* falso que passa por servidor de modo a ter acesso ilicitamente os dados dos outros ou comprometer os serviços do servidor.
- Negação de serviço: baseia-se na negação de serviço, negação essa que pode até encerrar o serviço.
- Repudiação: baseia-se na negação ou não autorização da transação por uma das partes envolvida na mesma.

Essas ameaças fazem com que tanto os consumidores como os fornecedores receiam em utilizar esta tecnologia para fazerem compras, preferindo que as compras/vendas sejam feitas nos estabelecimentos físicos.

Segundo o mesmo autor, os problemas de segurança no comércio eletrónico têm a ver com os seguintes aspetos:

- Privacidade: baseia-se no não acesso das informações de um utilizador a utilizadores não autorizados.
- Autenticidade: baseia-se na confirmação do utilizador, identificando-se como tal e provando que ele é realmente o utilizador em questão antes de confirmar qualquer transação.
- Autorização: baseia-se na atribuição de permissões de utilizador impedindo, deste modo, o acesso aos outros recursos pelo qual não está autorizado a utilizar.
- Não-Repudiação: baseia-se na negação de pedidos falsos de utilizadores com intenções maliciosas antes que o mesmo sendo que o mesmo precisa de se identificar.
- Integridade: consiste em manter a informação assim como o emissor o fez, não acrescentando, não eliminando e nem alterando nenhum dados.

16.2 Métodos de proteção

Para evitar que essas ameaças se concretizem várias são as medidas que podem ser adotadas (Filho (2000) apud Correia (2010)):

- Barreiras físicas (*firewall*): consiste em determinar regras no que diz respeito aos pacotes que devem entrar na rede e aos pacotes que devem sair na rede, portanto, um *firewall* bem configurado poderá limitar as oportunidades de o fraudulento infiltrar na rede.
- Criptografia: consiste em transformar a informação de sua forma legível para a forma ilegível de modo que só o recetor pretendido consiga ler o conteúdo da informação.
    - Criptografia simétrica: consiste na utilização de uma única chave que serve tanto para cifrar como também para decifrar.
    - Criptografia assimétrica: consiste na utilização de duas chaves (privada e pública), sendo a primeira só do conhecimento do dono e a segunda do conhecimento público.
- Protocolos de autenticação: consiste na verificação da identidade da pessoa, para saber se realmente é a pessoa que afirma ser, sendo que caso contrário, é ignorada e são tomadas as devidas medidas defensivas.

- *SSL* (*Secure Sockets Layer*): garante a segurança na transmissão de dados na *internet* através da utilização da criptografia da chave pública.
- *HTTPS* (*Secure Hipper Text Transfer Protocol*): garante a autenticidade, integridade, confidencialidade e certificação de dados permitindo a transmissão segura dos mesmos na *internet*.
- *SET* (*Secure Electronic Transaction*): garante a segurança nas transações eletrónicas pela *internet* através da encriptação de mensagens e utilização de assinaturas digitais.
- *S/MINE* (*Secure Multipurpose Internet Mail Exchange*): garante a segurança na transmição dos dados utilizando o algoritmo de encriptação *RSA*.
- *IPsec*: extensão do protocol *IP* garantindo a confidencialidade, integridade e autenticidade na transmição dos dados pela *internet*.

- Certificados Digitais: emitida pela Autoridade Certificadora, é um documento que comprova a identidade de uma pessoa bem como associa esta mesma pessoa a um par de chaves (pública e privada). De acordo com o mesmo autor, os certificados digitais possuem as seguintes informações:
  - Nome da entidade a quem a chave pertence;
  - Nome da entidade emissora do certificado digital;
  - Período de validade do certificado digital;
  - Chave pública certificada e o respetivo algoritmo;
  - Algoritmo utilizado na mesma assinatura digital;
  - Número de versão que indica o seu formato interno de acordo com as várias versões de certificado digital;
  - Número de serie, devendo ser único para todos os certificados digitais emitidos por uma dada entidade certificadora.
- Assinaturas Digitais: garante a autenticidade do emissor, a sua assinatura não pode ser manipulado, o documento assinado não pode ser alterado e a assinatura não é reutilizável.

- Selos Digitais: protegem os documentos mediante a utilização de carimbos cronológicos associando estes documentos a uma data e hora para que futuramente o emissor possa comprovar a existência de tais documentos.

17 Expansão do comércio eletrónico

A expansão do comércio eletrónico depende de três fatores importantes, sendo elas na óptica de Fernandes (2000):

- Criação de tecnologias de comercialização segura: sendo que o comércio eletrónico fornece uma receita muito considerável aos comerciantes, estes precisam adaptar as tecnologias de comercialização segura visto que:
    - Elevado número de transações são realizadas entra compradores e vendedores;
    - Geralmente, as partes envolvidas nas transações são desconhecidas;
    - As partes envolvidas nas transações estão, por vezes, separadas geograficamente;
    - O idioma do vendedor e do comprador pode ser diferente;
    - As transações podem ser de pequenas quantias até às quantias exorbitantes;
    - Os produtos comercializados podem ser físicos, digitais e serviços;

  Ainda as aplicações do comércio eletrónico não possuem as técnicas de soluções para todas as solicitações citadas acima, mas, no que diz respeito à segurança dos dados transmitidos durante o processo de transação, as tecnologias de suporte ao comércio eletrónico, normalmente, são agrupadas em quatro categorias citadas por Fernandes (2000):

    - Tecnologias baseadas em cartões de crédito: baseia-se na compra, com os já conhecidos, cartões de crédito.
    - Tecnologias baseadas em dinheiros eletrónicos: baseiam-se em dinheiros virtuais que podem ser adquiridos por meio dos cartões eletrónicos e que podem ser utilizadas na compra de outros produtos. Transação esta que é totalmente digital.

  - Tecnologias baseadas em cheques eletrónicos: baseia-se numa transação que utiliza as tecnologias idênticas aos baseados em cartões de crédito e dinheiros digitais, só que as transações efetuadas são vinculadas às contas bancárias.
  - Tecnologias baseadas em micro-pagamentos: são tecnologias que permitem grandes números de transações na ordem dos centavos, ou seja, micro-pagamentos.

- Regras comerciais claras: são regras previamente definidas que devem constar num sistema de comércio eletrónico, tais como *copyright*, taxas, privacidade do consumidor, entre outras regras.
- Reestruturação organizacional e económica: grandes mudanças na organização e no modo de operar das empresas bem como na economia das organizações são consequências das variações dos custos das transações praticadas no comércio eletrónico.

18 Restrições ao crescimento e à abrangência do comércio eletrónico

Segundo Cernev (2005), os estudiosos da TI depararam que existem barreiras que impedem a expansão do comércio eletrónico que atingem tanto a nível individual como também organizacional. São diversas as restrições à expansão e à abrangência do comércio eletrónico sendo de realçar as seguinte:

- Questões técnicas:
  - Dificuldade de acesso aos recursos de TI.
  - Limitações das atuais e novas tecnologias existentes.
  - Largura de banda não suficiente para as operações solicitadas.
- Questões económico-financeiras
  - Limitações quanto às formas de pagamento.
  - Elevado custo do *hardware*, *software* e dos provedores.
  - Fraca adoção a forma de pagamento com cartões de crédito.
- Questões socioculturais
  - Fraca experiência dos clientes e empresas em compras *online*.

  - Fraca experiência dos clientes quanto ao uso da *internet*.
  - Maior parte dos softwares de comércio eletrónico é em inglês.
- Questões relacionadas à adoção
  - Fraca flexibilidade nos negócios.
  - Elevado custo na conceção e manutenção do *site*.
  - Desagradável ou fraca experiência anterior.
- Questões relacionadas à confiança
  - Requisitos de segurança.
  - Requisitos de privacidade.
  - Existência de fraudes e *hackers*.
- Questões relacionadas à usabilidade
  - Ambiente de navegação pouco chamativa.
  - Processo de compra confuso e pouco fácil.
  - Dificuldade aos portadores de deficiência.
  - Páginas *web* pouco consistentes.
- Questões relacionadas a logística e distribuição
  - Custo de transporte agregado ao valor final do produto.
  - Demora na entrega dos produtos adquiridos.
  - Dificuldade na assistência técnica dos produtos comprados, principalmente quando estas foram compradas no exterior.
- Exclusão digital
  - Potenciais consumidores e produtores excluídos por causa do hábito do comércio tradicional, situações financeiras e da necessidade de aprender essas novas tecnologias (Cernev, 2005).

Cernev (2005), conclui afirmando que as categorias apresentadas acima podem ou não estar com a realidade, sendo que destaca que o mais importante é entender as restrições apresentadas.

Capítulo 3: Segurança no Comércio Eletrónico em Cabo Verde

No presente capítulo ter-se-á a oportunidade de avaliar, recorrendo à utilização da ferramenta *Acunetix v8*, a segurança dos *sites* de comércio eletrónico em Cabo Verde bem como ver o percurso do comércio eletrónico em Cabo Verde desde o surgimento da *internet* no país até o aproveitamento dessa tecnologia para a prática do comércio eletrónico.

1 Internet em Cabo Verde

O comércio eletrónico em Cabo Verde é uma prática recente visto que os serviços oferecidos pela *internet* também são recentes aqui em Cabo Verde.

De acordo com Dâmaso (2004), "*foi com a internet, mais concretamente com a web, que o comércio eletrónico conheceu a sua mais acentuada fase de desenvolvimento*", segundo a ANAC (2013), ela começou a ser comercializada em Cabo Verde em 1997 apesar de a sua instalação ser no ano de 1996 pela empresa CV Telecom. Nos anos de 1996 e 1997 foram considerados os anos experimentais pela ANAC sendo que nesses anos a adesão a esse serviço era de 474 clientes.

A mesma fonte realça que a instalação da internet em Cabo Verde foi feita em três fases:

- Na primeira fase deu-se, em 1998, com a instalação do primeiro *router* na cidade da Praia, foi utilizado a *DIAL-UP* analógico de 56Kbs e digital de 64Kbs. Nessa época, a adesão a esse serviço era de 1139 clientes,

- Na segunda fase, em 1999, houve uma expansão a nível nacional onde foram instaladas dois *routers*, um na cidade da Praia e outro em Mindelo. Na segunda fase a adesão a *internet* foi de 1654 clientes.
- Na terceira fase, a expansão foi ainda maior abrangendo todas as ilhas do arquipélago de Cabo Verde onde houve um aumento da amplitude da banda para *1Mbps*. A adesão nesse período aumentou para 1863 clientes.

Atualmente, devido às necessidades dos clientes e do avanço das tecnologias, melhores serviços da *internet* estão a ser oferecidos a população e, consequentemente, a adesão ao serviço da *internet* por todo o país aumentou de forma significante.

Em 1997, quando começou a ser comercializado a *internet*, a CV Telecom surgia como o único provedor de serviço da *internet* (ANAC (2013)), e que apesar de, hoje em dia, Cabo Verde contar com mais provedores da *internet*, como é o caso da CVWIFI (São Vicente), CABOCOM (Sal), T+, entre outros, a CV Telecom continua a ser o principal provedor de serviço da *internet* em Cabo Verde.

Segundo a ANAC (2010), sendo que a *internet* de banda larga tem estado a crescer de forma impressionante a nível mundial, e como Cabo Verde não poderia ficar atrás dessa evolução, a ANAC, em Janeiro de 2010, efetuou uma consulta pública cujo objetivo é introduzir no mercado cabo-verdiano o conceito de banda larga móvel visto que até o momento só se dispunha da *internet* banda larga fixa (*ADSL*).

No âmbito da consulta pública efetuada em 2010 pela ANAC, foram recebidas contribuições das seguintes entidades:

- Grupo CVTelecom – CVTelecom, CVMultimédia e CVMóvel
- MB Investimentos S.A.
- SITAM
- T+ Telecomunicações S.A.
- CABOCOM

Feita a consulta pública, a ANAC, em Agosto do mesmo ano, lançou um concurso público com o objetivo de licenciar três operadores de redes de comunicação de terceira geração, com acesso à *internet* de banda larga e através de aparelhos de telemóveis[2].

No dia 5 de Dezembro de 2011, a CVMóvel anunciou "*ter obtido uma licença para prestar serviços de telefonia móvel de terceira geração (3G)*"[3].

No âmbito do concurso público, que teve a participação de três operadores cabo-verdianos, a CVMóvel obteve o primeiro lugar, com mais de 98% de pontuação na fase de avaliação técnica, tendo em conta os critérios definidos pela ANAC[4].

Com a introdução da 3G em Cabo Verde, o número de assinantes da *internet* triplicou só no primeiro trimestre do ano 2012, segundo dados estatísticos das comunicações eletrónicas divulgados pela ANAC, sendo que esse ganho foi de 95.000 novos assinantes, o que representa 75% dos assinantes a usufruírem da banda larga móvel para acederem a *internet*, ultrapassando todos os outros tipos de acesso, nomeadamente a *Dial Up*, *ADSL* e a *Wireless*[5].

De acordo com ITU (2013), Cabo Verde ocupa o quarto lugar no ranking dos países africanos com maior taxa de penetração da utilização da *internet*, ficando somente atrás da República das Seicheles, República da Maurícia e África do Sul. No entanto, a mesma fonte realça que, a nível mundial, Cabo Verde ocupa a nonagésima sexta posição.

A taxa de penetração da utilização da *internet* em Cabo Verde tem estado a aumentar significativamente, passando de 1.6% em 2000 para 20% em 2008, e posteriormente, para 30% em 2010. Esse aumento deve-se a aposta nas praças digitais espalhadas por todo o país, nomeadamente o Projeto Konekta[6] bem como na facilidade da adesão do serviço e o preço acessível do mesmo.

No final do ano de 2011, Cabo Verde era o país africano de língua oficial portuguesa com a maior taxa de penetração do acesso à *internet* estando, igualmente, nos lugares cimeiros dos

[2] http://www.macauhub.com.mo/pt/2010/08/03/9535/, consultado a 30 de Julho de 2013
[3] http://www.macauhub.com.mo/pt/2011/12/05/empresa-de-cabo-verde-cvmovel-obteve-licenca-de-3g/, consultado a 30 de Julho de 2013
[4] http://www.macauhub.com.mo/pt/2011/12/05/empresa-de-cabo-verde-cvmovel-obteve-licenca-de-3g/, consultado a 30 de Julho de 2013
[5] http://legalafrica.wordpress.com/2012/07/26/cabo-verde-introducao-do-3g-triplica-o-numero-de-assinantes-de-internet/, consultado a 30 de Julho de 2013
[6] http://www.nosi.cv/index.php?option=com_content&view=article&id=469%3Acabo-verde-e-o-4o-pais-africano-com-a-maior-taxa-de-penetracao-do-uso-da-Internet&catid=36%3Adestaques1&Itemid=96&lang=pt, consultado a 30 de Julho de 2013

países de África com maior taxa de penetração da utilização da *internet*, de acordo com a revista *African Business*[7].

Estudos efetuados pela *African Business* revelam que Cabo Verde, em Dezembro de 2011, tendo uma população de 523 mil habitantes, possuía 148 mil pessoas que gozavam do acesso a *internet* que correspondia a uma taxa de penetração de, aproximadamente, 28%, tendo em conta que em Dezembro de 2000, somente 8 mil pessoas usufruíam desse serviço[8].

Segundo a *African Business*, "*a maior taxa de penetração no acesso à internet em África encontrava-se no final de 2011 em Marrocos com 49%, decorrente de uma população de 32 milhões de habitantes e 15,6 milhões de pessoas com acesso à internet*"[9].

Segundo ANAC, o gráfico abaixo retracta a evolução da *internet* em Cabo Verde[10]:

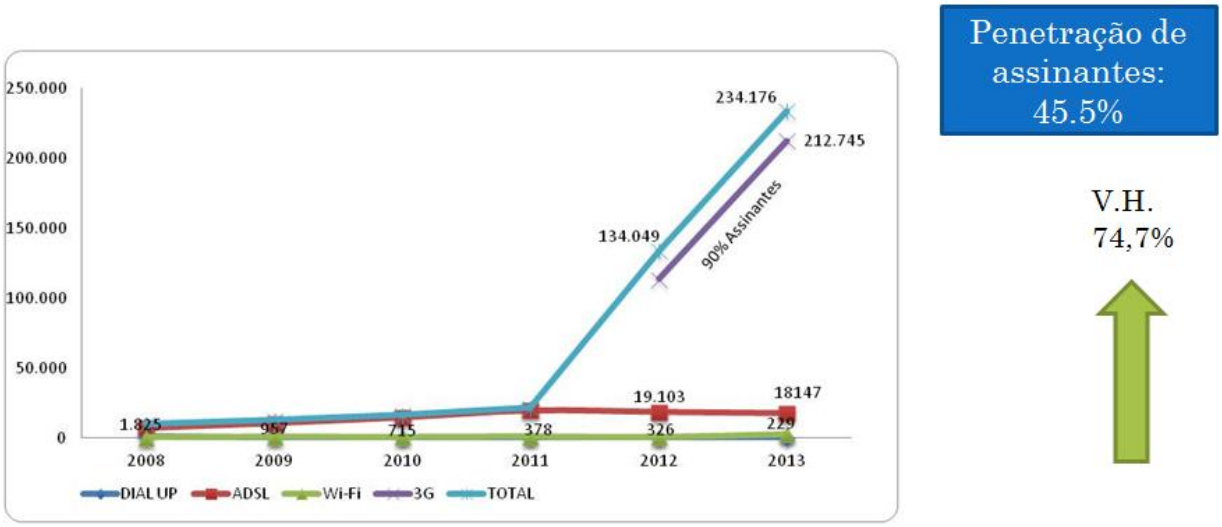

Figura 20 – Evolução da *internet* em Cabo Verde
Fonte - ANAC (2013)

De acordo com Da Rosa (2010), um dos principais problemas com a *internet* em Cabo Verde tem a ver com o seu elevado custo.

O mesmo autor realça que de 1997 a 2008 havia somente um único *ISP* (*Intenet Service Provider*) e, devido a sua monopolização no mercado cabo-verdiano, os preços estabelecidos

[7] http://www.macauhub.com.mo/pt/2012/11/13/cabo-verde-com-a-mais-elevada-taxa-de-penetracao-de-acesso-a-internet-na-africa-de-lingua-portuguesa/, consultado a 30 de Julho de 2013
[8] http://www.macauhub.com.mo/pt /2012/11/13/cabo-verde-com-a-mais-elevada-taxa-de-penetracao-de-acesso-a-internet-na-africa-de-lingua-portuguesa/, consultado a 30 de Julho de 2013
[9] http://www.macauhub.com.mo/pt/2012/11/13/cabo-verde-com-a-mais-elevada-taxa-de-penetracao-de-acesso-a-internet-na-africa-de-lingua-portuguesa/, consultado a 30 de Julho de 2013
[10] http://www.anac.cv/index.php?option=com_content&view=article&id=59&Itemid=56&lang=en, consultado a 30 de Julho de 2013

não favoreceriam ao que estavam dispostos a aderir a esse serviço. A esse elevado preço, fez com que entre 2006 e 2007 houvesse uma diminuição no número de assinantes da *internet* de 7475 para 7308.

Graças ao aparecimento de outros *ISPs* e de novos serviços como *Wi-Fi* e *internet* móvel *GPRS* fez com que, só no ano de 2008, os preços diminuíssem 4 vezes (Da Rosa (2010)).

Hoje em dia, os preços estão bem mais acessíveis e a qualidade de serviço melhorou bastante tendo em conta o lançamento desse serviço.

Outro dos grandes problemas relacionado com o custo, segundo Fernandes (2008) apud Da Rosa (2010), tem a ver com a utilização de *IP* estático sendo que a mesma apresentava-se como uma alternativa bastante dispendiosa que seria mais viável alojar os seus serviços fora de Cabo Verde.

A tabela abaixo demonstra o custo das linhas dedicadas tendo em conta a sua velocidade:

Velocidade	Mensalidade
128 Kbs	548,86 €
256 Kbs	1.254,55 €
512 Kbs	1.881,82 €
1024 Kbs	3.502,27 €
2048 Mbs	5.854,55 €
4 Mbs	10.454,55 €
8 Mbs	16.831,82 €
16 Mbs	27.099,23 €
32 Mbs	70.243,91 €

Tabela 2 – Linhas dedicadas (serviços *IP*) 2008 – CV Multimédia
Fonte – Da Rosa (2010)

Em relação à tabela acima, atualmente houve uma redução nos custos das linhas dedicadas tendo em conta a sua velocidade, embora os preços, ainda, têm estados elevados conforme a tabela abaixo:

Velocidade	Mensalidade CVE	Mensalidade EURO
28 Kb/s	23.000,00	208,59
64 Kb/s	46.000,00	417,18
128 Kb/s	80.500,00	730,06
256 Kb/s	109.250,00	990,79
512 Kb/s	138.000,00	1.251,53
1 Mb/s	207.000,00	1.877,30
2 Mb/s	385.250,00	3.493,86

Tabela 3 – Linhas dedicadas (serviços *IP*) – CV Multimédia
Fonte – http://www.cvmultimedia.cv/serviço-ip

2 Comércio eletrónico em Cabo Verde

Segundo Correia (2010), sendo o comércio eletrónico todo o processo de compra, venda e/ou prestação de serviços efetuados eletronicamente, a implementação de meios capazes de efetuar pagamentos eletrónicos faria com que o comércio eletrónico fosse mais fácil.

De acordo com Correia (2010) "*A única entidade responsável para a gestão e controlo dos sistemas eletrónicos de pagamentos nesse país é a SISP (Sociedade Interbancária e Sistemas de Pagamentos), que foi criada em 1999 com a principal missão de gerir a rede interbancária nacional*", sendo que Cabo Verde é um país recente no que diz respeito a prática do comércio eletrónico, e sendo que o comércio eletrónico definido como toda e qualquer troca, venda ou compra de produtos/serviços utilizando meios eletrónico, pode-se dizer que, para Cabo Verde, o principal meio utilizado para efetuar o comércio eletrónico é o pagamento de produtos/serviços através de cartões de débito/crédito nas máquinas *POS* (*Point of Service / Point of Sale*) localizados nos estabelecimentos onde se efetua as compras.

Figura 21 – Cartão Vinti4 e máquina *POS*
Fonte - Correia (2010)

Há, também, outros modos em que se possa efetuar o comércio eletrónico em Cabo Verde, nomeadamente utilizando a *internet banking*, como é o caso do pagamento de serviços (faturas) no *internet banking* do BCA, entre outros bancos, apesar dessa prática ainda não ser tão corrente entre os cabo-verdianos, onde pode-se escolher a entidade a efetuar o pagamento, a referência da fatura e o montante a ser pago bem como o pagamento de produtos/serviços em outros *sites* que praticam o comércio eletrónico (casa do cidadão, entre outros). A figura abaixo ilustra o exemplo de um pagamento de serviços utilizando o *site* do BCA:

Figura 22 – Interface para Pagamento de Serviços
Fonte - https://bcadirecto.bca.cv/

Convém referir que entre as formas mais utilizadas de efetuar as operações (compras) eletronicamente são:

- Cartão de débito;
- Depósito ou transferência;
- Cartão de crédito;
- *Internet banking*.

Atualmente, com o avanço das tecnologias de informação e telecomunicação, bem como com a necessidade de expandir o negócio sem que haja grandes investimentos, em Cabo Verde, assim como noutros países, surgiu a necessidade de dinamizar o comércio através do comércio eletrónico onde os comerciantes conseguem expor os seus produtos eletronicamente e onde os clientes poderão comprá-los, também, eletronicamente.

Em Cabo Verde, existem *sites* de comércio eletrónico onde os clientes poderão ver e comprar produtos eletronicamente sem a necessidade de aceder outros modos de pagamento que não seja no próprio *site*, como é o caso do *site* http://www.recortes.cv/, mas também há *sites* onde podem-se efetuar a mesma coisa mas só que no ato do pagamento pode-se escolher entre o pagamento *online*, utilizando o cartão de crédito, bem como efetuar uma transferência para a conta do vendedor e enviar o comprovativo do depósito para o mesmo para que se possa fazer o levantamento do produto comprado.

O fenómeno do comércio eletrónico ainda é uma prática não muito explorada pelos cabo-verdianos onde a causa poderá ser a não confiança nas aplicações *web* visto que, onde há

transação de dinheiro, além do receio, o cliente estará perante uma aplicação *web* onde poderá ou não estar vulnerável a certos tipos de ataques.

Para tal, existem ferramentas tais como *Acunetix Web Vulnerability*, *Nessus*, entre outros, que permitem verificar a existência de vulnerabilidades nas aplicações *web*.

3 Verificação de vulnerabilidades com *Acunetix Web Vulnerability*

De acordo com Viegas (2008), *Acunetix Web Vulnerability* é uma ferramenta que permite verificar a existência de vulnerabilidades que podem ser exploradas através de técnicas malícias praticadas pelos *hackers* para a obtenção de dados de forma indevida, bem como essas vulnerabilidades podem ser exploradas pelos responsáveis da segurança informática com o objetivo de identificar possíveis falhas nos seus sistemas e protege-los de tais falhas.

Foi optada pela utilização do *Acunetix Web Vulnerability v8*, por ser uma ferramenta de fácil utilização, além de ser grátis, bem como a mesma apresenta dados de relatório de fácil compreensão.

Tal ferramenta permite verificar se a aplicação *web* em estudo encontra-se vulnerável a *SQL Injection*, *XSS* (*Cross Site Scripting*), *CSRF* (*Cross Site Request Forgery*), entre outras.

Para a procura de vulnerabilidades nos *sites* de comércio eletrónico em Cabo Verde, foi levada em conta a lista abaixo de *sites* cabo-verdianos que praticam o comércio eletrónico:

Entidade	Endereço
Casa do Cidadão	https://portoncv.gov.cv/
Transportes Aéreos de Cabo Verde (TACV)	http://www.flytacv.com/
Banco Comercial do Atlântico (BCA)	https://bcadirecto.bca.cv/
Banco Interatlântico	https://binanet.bi.cv/
Caixa Económica de Cabo Verde	https://caixanetparticulares.caixa.cv/
Banco Angolano de Investimentos	https://www.bancobai.cv/wps/portal/baiparticulares/BAIParticulares/login/
Balcão Virtual da CMP	https://lojacmp.com/

Tabela 4 – Endereços de entidades que praticam o comércio eletrónico

O motivo da escolha das empresas acima para procurar vulnerabilidades tem a ver em perceber como essas referidas empresas, sendo que elas lidam com o comércio eletrónico, protegem as informações/dados que transitam no seus *sites* bem como verificar, entre empresas do mesmo ramo de atividade, as diferenças tendo em conta as vulnerabilidades encontradas.

O facto do leque dos *sites* escolhidos ser maioritariamente dos bancos tem a ver com o facto de Cabo Verde ter adotado recentemente ao fenómeno do comércio eletrónico sendo que ainda há poucos *sites* de comércio eletrónico em Cabo Verde tendo em conta que a maioria é de bancos que por sua vez são instituições que devem manter todo e qualquer tipo de informações dos clientes salvaguardados da melhor maneira possível sem, no entanto, menosprezar que os outros *sites* de comércio eletrónico deverão zelar ao máximo pela segurança das informações que transitam nos mesmos.

O resultado obtido da procura de vulnerabilidades a partir da ferramenta *Acunetix Web Vulnerability v8* tendo em conta as vulnerabilidades tais como *SQL Injection*, *XSS* e *CSRF*, são apresentados nas tabelas abaixo seguindo os seguintes critérios:

- Presença de vulnerabilidades;

	Principais Vulnerabilidades Pesquisadas		
	SQL Injection	*XSS*	*CSRF*
Casa do Cidadão	Não	Não	Não
TACV	Sim	Sim	Sim
BCA	Não	Não	Não
BI	Não	Sim	Sim
CECV	Sim	Não	Sim
BAI	Sim	Sim	Sim
Balcão Virtual da CMP	Sim	Sim	Sim

Tabela 5 – Presença de vulnerabilidades

- Quantidade de vulnerabilidades por site analisado;

	Principais Vulnerabilidades Pesquisadas		
	SQL Injection	*XSS*	*CSRF*
Casa do Cidadão	0	0	0
TACV	58	17	2
BCA	0	0	0
BI	0	2	2
CECV	2	0	1
BAI	133	135	135
Balcão Virtual da CMP	28	23	21

Tabela 6 – Quantidade de vulnerabilidades por *site*

4 Análise do resultado obtido da procura de vulnerabilidades

Feita a procura de vulnerabilidades nos sites de comércio eletrónico acima indicados com a utilização da ferramenta *Acunetix*, torna-se necessário efetuar uma análise sobre o resultado obtido tendo em conta os critérios definidos anteriormente.

4.1 Presença de vulnerabilidades

Tendo em conta a presença de vulnerabilidades nos sites estudados, pode-se contar que, exceto o BCA, todas as vulnerabilidades acima referidas se encontram presentes nos sites analisados.

De acordo com o gráfico abaixo, pode-se analisar a ocorrência, em percentagem, das vulnerabilidades nos sites de comércio eletrónico estudados.

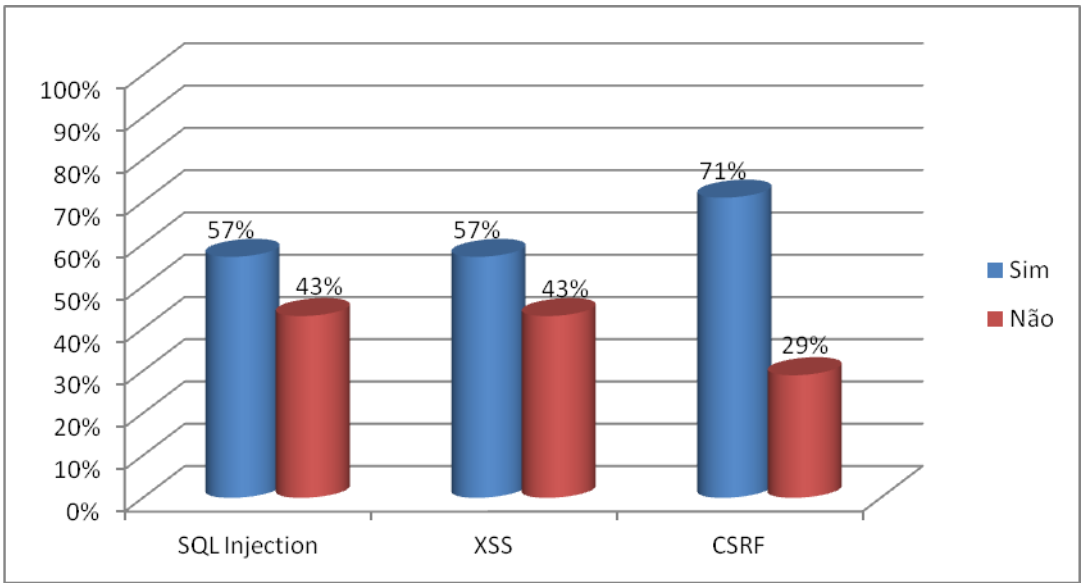

Figura 23 – Presença de vulnerabilidades (%)

Tendo em conta a figura 24, pode-se contar que a maioria dos sites de comércio eletrónico analisados possui as principais vulnerabilidades pesquisadas, onde as consequências para cada tipo são:

- *SQL Injection*
    - O *hacker* poderá efetuar o uso da sua técnica para manipular a entrada utilizando comandos *SQL* visto que não a uma validação dos dados de entradas para que possam ser suprimidos os caracteres perigosos, comprometendo, deste modo, a integridade dos dado do sistema e/ou expondo informações consideradas confidenciais para a organização atacada.

      De acordo com OWASP (2007), "*Caso uma entrada de usuário seja fornecida a um interpretador sem validação ou codificação, a aplicação é vulnerável. Verifique se a entrada de usuário é fornecida à queries dinâmicas, como por exemplo*":

      ```
      $sql = "SELECT * FROM table WHERE id = '" . $_REQUEST['id'] . "'";
      ```

- *XSS*
    - O *hacker* poderá enviar códigos maliciosos, podendo ser em forma de *script*, onde o utilizador mesmo sem saber executará o mesmo fazendo com que o *hacker* lhe roube algumas informações podendo prejudicar o utilizador visto

que o hacker agirá como se fosse o utilizador. Informações essas que podem ser o *cookie* da sessão onde o invasor poderá assumir a conta e agir como se fosse o utilizador legitimo.

De acordo com Brandão e da Rosa (2014), os códigos abaixo mostram uma aplicação vulnerável a *XSS* onde é roubada o id da sessão da vítima:

```
(String) page += "<input name='creditcard' type='TEXT' value='" +
request.getParameter("CC") + "'>";
```

Onde o *hacker* altera o parâmetro "CC" no seu browser para:

```
(String) page += "<input name='creditcard' type='TEXT' value='" +
request.getParameter("CC") + "'>";
```

Agora, o *hacker* poderá agir como se fosse a pessoa autenticada.

- *CSRF*
    - O *hacker* poderá roubar sessões através de *script* e informações confidenciais sendo que os mesmos carecem de validações nos dados de entradas e possíveis divulgações de informações confidenciais tendo em conta que os formulários presentes no site armazenam, com a permissão do utilizador, as senhas e outras informações o que poderá ser extraviado se o invasor tiver acesso à máquina.

      De acordo com OWASP (2007), "*caso um banco permita sua aplicação a processar requisições, como a transferência de fundos, um ataque similar pode permitir*":

```
<img
src="http://www.example.com/transfer.do?frmAcct=document.form.frmAcct
&toAcct=4345754&toSWIFTid=434343&amt=3434.43">
```

Ainda, tendo em conta a presença das principais vulnerabilidades pesquisadas nos *sites* de comércio eletrónico acima referida, pode-se constar que:

- *SQL Injection* ocorre em 4 dos 7 *sites* analisados:
    - Sendo que na maioria dos sites de comércio eletrónico analisados presencia a vulnerabilidade do tipo *SQL Injection*, os mesmos correm sérios riscos de, por

parte dos *hackers*, aceder indevidamente a informações nas base de dados desses *sites*.

- *XSS* ocorre em 4 dos 7 *sites* analisados:
    - A maioria dos *sites* de comércio eletrónico analisados presencia a vulnerabilidade do tipo XSS, pelo qual correm riscos de serem roubadas informações pessoais, sessões, modificar/desfigurar o *site*, entre outras malícias por parte dos *hackers*.
- *CSRF* ocorre em 5 dos 7 *sites* analisados:
    - Dos sites de comércio eletrónico analisados, somente 1 está imune a este tipo de vulnerabilidade, que é o caso do BCA, sendo que nos outros casos há o risco dos *hackers*, através de suas técnicas, forçar a sua entrada no sistema fazendo-se passar por um utilizador autenticado realizando, deste modo, ações em nome da vitima.
- *SQL Injection* e *XSS* ocorrem em 3 dos 7 *sites* analisados:
    - A maioria dos *sites* de comércio eletrónico analisados apresenta essas duas vulnerabilidades em simultâneo o que faz com que o *hacker* tenha mais possibilidades de explorar e, por consequente, apropriar-se de informações de forma ilegal e modificar o conteúdo apresentado nos *sites*.
- *SQL Injection* e *CSRF* ocorrem em 4 dos 7 *sites* analisados:
    - A maioria dos *sites* de comércio eletrónico analisados apresenta essas duas vulnerabilidades em simultâneo o que faz com que o *hacker* tenha mais possibilidades de explorar e, por consequente, apropriar-se de informações de forma ilegal, modificar o conteúdo apresentado nos *sites* bem como fazer-se passar por utilizador autenticado realizando ações em nome da vítima.
- *XSS* e *CSRF* ocorrem em 5 dos 7 *sites* analisados:
    - A maioria dos *sites* de comércio eletrónico analisados apresenta essas duas vulnerabilidades em simultâneo o que faz com que o *hacker* tenha mais possibilidades de explorar e, por consequente, modificar o conteúdo apresentado nos *sites* bem como fazer-se passar por utilizador autenticado realizando ações em nome da vítima.

- *SQL Injection*, *XSS* e *CSRF* ocorrem em 4 dos 7 *sites* analisados:
    - Dos 7 *sites* de comércio eletrónico analisados, 4 apresentam todos os principais tipos de vulnerabilidades, o que representa um grande risco e ponto do *hacker* poder assumir o *site* bem como aceder a todas as informação, podendo divulga-las, extravia-las ou mesmo para o uso próprio por parte dos *hackers*.

4.2 Quantidade de vulnerabilidades por *site* analisado

Tendo em conta a quantidade de vulnerabilidades nos *sites* estudados, pode-se verificar que, exceto o BCA, todos os *sites* acima analisados possuem inúmeras as vulnerabilidades.

De acordo com o gráfico abaixo, pode-se analisar a ocorrência, quantidade/tipo, das vulnerabilidades nos *sites* de comércio eletrónico estudados.

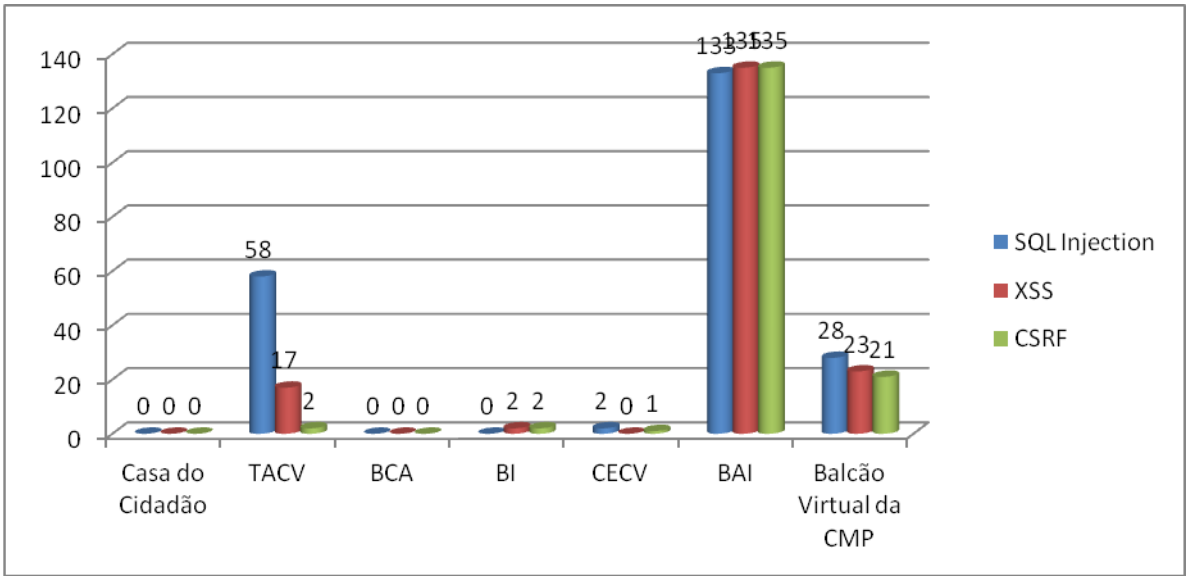

Figura 24 – Quantidade de vulnerabilidades por tipo

De acordo com a figura 25, pode-se verificar que, das empresas em que o seu *site* de comércio eletrónico foi analisado utilizando a ferramenta *Acunetix v8*, a que apresenta o maior número de vulnerabilidade é o BAI (403) enquanto o BCA e a Casa do Cidadão não apresentam nenhuma vulnerabilidade sendo a mesma considerada como um *site* seguro.

Ainda tendo em conta a figura 25, dos tipos de vulnerabilidades analisadas, a que apresenta o maior número de ocorrência é *SQL Injection* (221), num total de 559 vulnerabilidades encontradas, sendo que a mesma, segundo OWASP (2007), consiste na inserção de dados em forma de comandos *SQL* por parte do *hacker* com o intuito de aproveitar de forma indevida de dados ou informações.

O gráfico abaixo apresenta a ocorrência, quantidade/empresa, das vulnerabilidades nos *sites* de comércio eletrónico estudados.

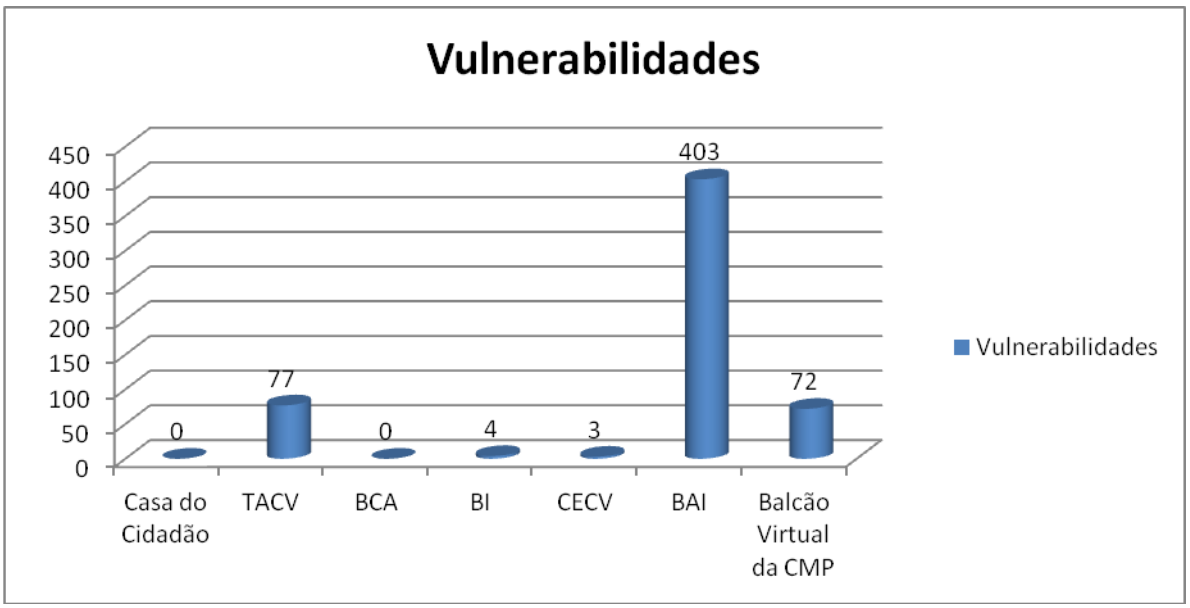

Figura 25 – Quantidade de vulnerabilidades por empresa

De acordo com a figura 26, pode-se verificar o número de vulnerabilidades ocorridas em cada *site* de comércio eletrónico analisado sendo que a empresa que possui o maior número de vulnerabilidades é o BAI (403) enquanto o BCA e a Casa do Cidadão (0) não apresentam nenhuma vulnerabilidade. Convém realçar que as empresas BI e CECV apresentam um número de vulnerabilidades relativamente baixo, 4 e 3 respetivamente.

Ainda tendo em conta a figura 26, num total de 559 vulnerabilidades encontradas após a verificação em todos os *sites* analisados, pode-se afirmar que, em média, cada *site* apresenta 80 vulnerabilidades o que representa um número elevado tendo em conta que os *hackers* são dotados de técnicas que, por mínima falha, podem aproveitar para aceder e divulgar informações indevidas, modificar *sites*, entre outras malícias.

5 Recomendações sobre o resultado obtido da procura de vulnerabilidades

Feita a análise da procura de vulnerabilidades nos *sites* de comércio eletrónico acima indicados com a utilização da ferramenta *Acunetix v8*, torna-se necessário efetuar recomendações a fim de proteger os *sites*:

- Banco Comercial do Atlântico (BCA):

- Sendo um *site* seguro, o que foi verificado após a procura de vulnerabilidades, nada se tem a recomendar a não ser uma atualização periódica das políticas de segurança visto que a informática é uma ciência dinâmica e novas formas de invadir os *sites* estão sempre a serem pesquisadas.

- Transportes Aéreos de Cabo Verde (TACV):
  - Sendo um *site* que apresentou muitas vulnerabilidades, *SQL Injection* e *XSS*, após a procura de vulnerabilidades, recomenda-se que seja feita validações nos dados de entrada, visto que esse é o principal motivo do *site* ser vulnerável, e converter os caracteres considerados perigosos por caracteres inofensivos impedindo, deste modo, a *SQL Injection* e *XSS*.

- Casa do Cidadão:
  - Tal como o *site* da BCA, sendo um *site* seguro, o que foi verificado após a procura de vulnerabilidades, nada se tem a recomendar a não ser uma atualização periódica das políticas de segurança visto que a informática é uma ciência dinâmica e novas formas de invadir os *sites* estão sempre a serem pesquisadas.

- Banco Interatlântico (BI):
  - Sendo um *site* seguro, o que foi verificado após a procura de vulnerabilidades, o que se recomenda é uma atualização periódica das políticas de segurança visto que a informática é uma ciência dinâmica e novas formas de invadir os *sites* estão sempre a serem pesquisadas e a eliminação das quatros vulnerabilidades de média severidade de forma a prevenir que as mesmas causem danos maiores sendo que as mesmas podem ser extintas utilizando métodos eficazes na validação dos dados de entrada.

- Caixa Económica de Cabo Verde (CECV):
  - Sendo um *site* razoavelmente seguro, o que foi verificado após a procura de vulnerabilidades, o que se recomenda é uma atualização periódica das políticas de segurança visto que a informática é uma ciência dinâmica e novas formas de invadir os *sites* estão sempre a serem pesquisadas e a eliminação das duas vulnerabilidades de alta severidade e das quatros vulnerabilidades de média severidade de forma a prevenir que as mesmas causem danos maiores sendo

que as mesmas podem ser extintas utilizando métodos eficazes na validação dos dados de entrada.

- Banco Angolano de Investimentos (BAI):
    - Tal como o *site* da TACV e Balcão Virtual da CMP, apresentou muitas vulnerabilidades, *SQL Injection*, *XSS* e *CSRF*, após a procura de vulnerabilidades, recomenda-se que seja feita validações nos dados de entrada, visto que esse é o principal motivo do *site* ser vulnerável, e converter os caracteres considerados perigosos por caracteres inofensivos impedindo, deste modo, a *SQL Injection* e *XSS*.
- Balcão Virtual da CMP:
    - Tal como o *site* da TACV, apresentou muitas vulnerabilidades, *SQL Injection* e *XSS*, após a procura de vulnerabilidades, recomenda-se que seja feita validações nos dados de entrada, visto que esse é o principal motivo do *site* ser vulnerável, e converter os caracteres considerados perigosos por caracteres inofensivos impedindo, deste modo, a *SQL Injection* e *XSS*.

Conclusão

O comércio eletrónico surgiu da necessidade do vendedor expandir o seu negócio sem que sejam gastos elevados recursos económicos. Surgiu de forma a dinamizar, expandir e/ou internacionalizar o comércio tradicional, sendo que as compras e vendas ficaram facilitadas aos clientes onde os mesmos poderiam efetuar as suas compras sem dirigirem às lojas físicas.

Por seu lado, as lojas virtuais deverão ter um aspeto agradável e organizado de modo que o consumidor possa encontrar os itens desejados sem dificuldades bem como nas referidas lojas virtuais efetuarem compras de maneira mais simplificada.

Tendo em conta que a *internet* é um ambiente suscetível a ataques, convém realçar que um dos aspetos mais importante do comércio eletrónico, além de efetuar compras e vendas, é garantir a segurança dos dados que circulam no momento da compra/venda.

A segurança, por sua vez, é dos aspetos mais importantes visto que a relutância em efetuar compras na *internet* tem a ver com a insegurança instalada nos consumidores visto que os mesmos têm duvidas se o *site* é seguro.

Tendo em consideração que o comércio eletrónico é um negócio muito rentável, o mesmo tem que ser aceite pelos consumidores de modo que possam sentir satisfeitos e seguros durante o ato da compra de produtos eletronicamente para que se possa sentir satisfeito pelo investimento feito e, novamente, voltar a efetuar compras e, quem sabe, sugerir o mesmo *site* para outros consumidores.

Assim como qualquer tipo de negócio, o comércio eletrónico tem as suas vantagens e desvantagens, sendo que cabe ao dono da loja virtual explorar ao máximo as vantagens oferecidas bem como tirar proveito das desvantagens a ponto de transformá-las em vantagens para o seu negócio.

Sendo o comércio eletrónico um fenómeno mundial, Cabo Verde também está inserido no grupo de países que praticam o comércio eletrónico. Embora encontra-se ainda numa fase inicial no que se refere a este fenómeno, Cabo Verde possui muitas empresas que já aderiram ao comércio eletrónico utilizando site amigáveis e seguros de forma a facilitar os processos de compra e vendas para os clientes, bem como o processo de pagamento nos mesmos.

Os clientes em Cabo Verde vão aderindo lentamente ao comércio eletrónico em detrimento do comércio tradicional sempre que possível, embora ainda este número apresentar-se bastante reduzido por causa do recente impacto do comércio eletrónico no país.

Os *sites* de comércio eletrónico em Cabo Verde apresentam uma interface amigável onde, a cada dia que passa, a mesma é constantemente melhorada com o objetivo de melhor servir o cliente.

Os mesmos aparentam ser seguros, podendo os clientes efetuarem os respetivos pagamentos sem receios, embora, é importante continuar a investir na segurança dos *sites* de modo a atrair os consumidores a aderirem a prática do comércio eletrónico com maior frequência

Embora o fenómeno de comércio eletrónico ainda seja recente aqui em Cabo Verde, de acordo com ITU (2013), Cabo Verde ocupa o quarto lugar no ranking dos países africanos com maior taxa de penetração da utilização da internet.

Resumindo, segundo Felipini (2010), "*tanto para os comerciantes tradicionais quanto para os empreendedores da nova economia, o e-commerce representa novos desafios e, principalmente, novas oportunidades de se chegar até o cliente de forma rápida, ágil e com um custo sensivelmente menor*", sempre prezando pela segurança do mesmo, sendo que os *sites* seguros atraem muitos consumidores e fazem com que haja um aumento na adesão dessa nova prática.

Bibliografia

ANAC (2010), *Relatório de consulta pública sobre introdução de redes de comunicações móveis de terceira e quarta geração em Cabo Verde*. Disponível em http://www.portaldoconhecimento.gov.cv/bitstream/10961/1982/2/relatorioconsultapublica3G.pdf, consultado a 30 de Março de 2013.

ANAC (2013), *Internet – Descrição*. Disponível em http://www.anac.cv/index.php?option=com_content&view=article&id=76&Itemid=56&lang=pt, consultado a 08 de Abril de 2013.

Brain, M. (2008). *Como funciona o comércio eletrónico*. Disponível em http://informatica.hsw.uol.com.br/comercio-eletronico5.htm, consultado a 19 de Março de 2012.

Brandão, A. P. & da Rosa, I. B. (2014). *Segurança nos sites governamentais de Cabo Verde.* Consultado a 10 de Setembro de 2014.

Campos, T. P. (2006). *Como se faz Comércio Eletrónico*. Disponível em http://www2.dc.uel.br/nourau/document/?view=517, consultado a 25 de Março de 2012.

Cernev, A. K. (2005). *Restrições ao crescimento e à abrangência do comércio eletrónico*. Disponível em http://www.adrian.cernev.com.br/arquivos/Restri%C3%A7%C3%B5es%20ao%20Com%C3%A9rcio%20Eletr%C3%B4nico.pdf, consultado a 25 de Março de 2012.

Correia, J. C. V. (2010). *Comércio Eletrónico em Cabo Verde*. Monografia de Licenciatura, Universidade Jean Piaget de Cabo Verde. Praia. Disponível em http://bdigital.cv.unipiaget.org:8080/jspui/handle/10964/357, consultado a 25 de Abril de 2012.

Da Rosa, I. B. O. (2010). *Construção e utilização de bibliotecas digitais: Contextos de acesso deficitário a material impresso e a tecnologia de informação e comunicação*. Tese de Doutoramento, Universidade de Santiago de Compostela. Galiza.

De Paula, D. D. R. (2011). *Gestão da informação na Fiocruz.* Disponível em http://www.ci.uff.br/ppgci/arquivos/Dissert/Diss_DanuziaPaula.pdf, consultado a 12 de Setembro de 2014.

Felipini, D. (2011). *ABC do E-commerce*. Disponível em http://vencergt.com/wp-content/uploads/2010/07/abc-4segredos-cli.pdf, consultado a 25 de Abril de 2012.

Felz, J. (2007). *Uma Breve História da Internet*. Disponível em http://ciberjor.files.wordpress.com/2007/09/historia-da-internet.pdf, consultado a 25 de Abril de 2012.

Fernandes, J. H. C. (2000). *Ciberespaço: Modelos, Tecnologias, Aplicações e Perspectivas; da Vida Artificial à Busca por uma Humanidade Auto-Sustentável*. Disponível em http://www.cic.unb.br/~jhcf/MyBooks/ciber/Ciber2000.pdf, consultado a 31 de Março de 2012.

International Telecommunication Union ITU (2013). *Measuring the Information Society*. Disponível em http://www.itu.int/en/ITU-D/Statistics/Documents/publications/mis2013/MIS2013-exec-sum_E.pdf, consultado a 10 de Dezembro de 2013

Junior, E. A. (2007). *Comércio Eletrónico*. Disponível em http://www.consulting.com.br/edsonalmeidajunior/admin/downloads/comercioeletronico.pdf, consultado a 19 de Março de 2012.

Laureano, M. A. P. (2005). *Gestão de Segurança da Informação*. Disponível em http://www.mlaureano.org/aulas_material/gst/apostila_versao_20.pdf, consultado a 14 de Agosto de 2012.

Luciano, E. M. (2004). *Consolidação de Componentes de Modelo de Negócios para o Comércio Eletrónico de Produtos Virtuais*. Disponível em http://www.ea.ufrgs.br/professores/hfreitas/files/orientacao/doutorado/tese/pdf/06_dout_tese_edimara.pdf, consultado a 26 de Abril de 2012.

OWASP (2007). *As 10 vulnerabilidades de segurança mais críticas em aplicações WEB*. Disponível em https://www.owasp.org/images/4/42/OWASP_TOP_10_2007_PT-BR.pdf, consultado a 16 de abril de 2013.

Reis, B. & Mota, J. C. & de Oliveira, P. P. B. *Classificação da Informação*. Disponível em http://www.lyfreitas.com.br/ant/artigos_mba/artclassinfo.pdf, consultado a 10 de Setembro de 2014.

Rocha, R. S. (2005). *Sites de Comércio Eletrónico e a Responsabilidade pela Intermediação no Ambiente Virtual*. Disponível em

http://www.lume.ufrgs.br/bitstream/handle/10183/5437/000515351.pdf?sequence=1, consultado a 31 de Março de 2012.

Santos, E. (2005). *Comercio Eletrónico.* Disponível em http://www.ebah.com.br/content/ABAAAA9iEAK/comercio-eletronico, consultado a 19 de Março de 2012.

Silva, P. T. & Carvalho, H. & Torres, C. B. (2003). *Segurança dos Sistemas de Informação*. Disponível em http://www.centroatl.pt/titulos/si/imagens/excerto-ca-seguranca-si.pdf, consultado a 26 de Agosto de 2012.

Silva, T. E. & Tomaél, M. I. (2007). *A gestão da informação nas organizações*. Disponível em http://www.uel.br/revistas/uel/index.php/informacao/article/download/1806/1540, consultado a 01 de Setembro de 2014.

Tigre, P. B. (1999). *"Comércio Eletrónico e Globalização: desafios para o Brasil" in Lastres, Helena et al, Informação e Globalização na Era do Conhecimento. Rio de Janeiro: Campus, pp. 84-104.* Disponível em http://www.liinc.ufrj.br/pt/attachments/055_saritalivro.pdf, consultado a 6 de Abril de 2012.

Tribunal de Contas da União TCU (2008). *Boas Práticas em Segurança da Informação.* 3ª edição, Brasília. Disponível em http://portal2.tcu.gov.br/portal/pls/portal/docs/2059160.PDF, consultado a 12 de Setembro de 2014

Viegas, A. L. (2008). *Segurança de Aplicações WEB: Hardering nos Serviços baseados em softwares livre*. Disponível em http://www.nogueira.eti.br/profmarcio/obras/Alberto%20Seguranca%20de%20Aplicacoes%20Web.pdf, consultado a 15 de Abril de 2013.